

CLI, livre 1 : Guide de configuration de l'interface de ligne de commande pour l'exploitation générale de la gamme Cisco Secure Firewall ASA, 9.19

Dernière modification : 2026-03-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. Tous droits réservés.

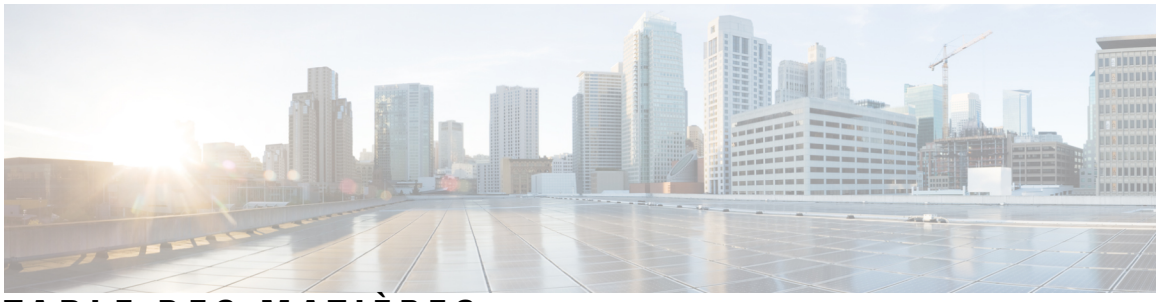


TABLE DES MATIÈRES

PRÉFACE

À propos de ce guide lv

Objectifs du document lv

Documentation associée lv

Conventions de document lv

Communications, services et renseignements supplémentaires lvii

PARTIE I

Mise en route de l'ASA 59

CHAPITRE 1

Introduction à Secure Firewall ASA 1

Compatibilité matérielle et logicielle 1

Compatibilité VPN 1

Nouvelles fonctionnalités 1

Nouvelles fonctionnalités dans l'ASA 9.19(1) 2

Présentation fonctionnelle du pare-feu 4

Présentation de la politique de sécurité 5

Autorisation ou refus de trafic avec critères d'accès 5

Application de la NAT 5

Protection contre les fragments IP 5

Application du filtrage HTTP, HTTPS ou FTP 5

Application de l'inspection des applications 5

Application des politiques de QoS 5

Application des limites de connexion et de la normalisation TCP 6

Activation de la détection des menaces 6

Présentation du mode pare-feu 6

Présentation de l'inspection dynamique 7

Présentation fonctionnelle VPN 8

Présentation du contexte de sécurité 8
Présentation de la mise en grappe d'ASA 9
Services spéciaux et existants 9

CHAPITRE 2 **Pour commencer 11**

Accéder à la console de l'interface de commande en ligne 11
Accéder à la console de l'ISA 3000 11
Accéder à la console du mode plateforme de Firepower 2100 12
Accéder à la console Firepower 1000, 2100 en mode appareil et Secure Firewall 3100 15
Accéder à la console ASA sur le Châssis Firepower 4100/9300 16
Configurer l'accès ASDM 18
Utiliser la configuration d'usine par défaut pour l'accès ASDM 18
Personnaliser l'accès ASDM 19
Démarrer ASDM 21
Configurations d'usine par défaut 22
Rétablir les valeurs par défaut de la configuration 23
Restaurer la configuration du déploiement de l'ASA virtuel 26
Configuration par défaut de Firepower 1010 26
Configuration par défaut de Firepower 1100 28
Configuration par défaut du mode plateforme de Firepower 2100 29
Configuration par défaut du mode appareil de Firepower 2100 30
Configuration par défaut de Secure Firewall 3100 32
Configuration par défaut de Châssis Firepower 4100/9300 33
Configuration par défaut d'ISA 3000 33
Configuration du déploiement ASA virtuel 35
Régler le Firepower 2100 en mode appareil ou plateforme 37
Travailler avec la configuration 39
À propos de la configuration de démarrage et de la configuration en cours d'exécution 39
Enregistrer les modifications de configuration 40
Enregistrer les modifications de configuration en mode de contexte unique 40
Enregistrer les modifications de configuration en mode de contexte multiple 40
Copier la configuration de démarrage dans la configuration en cours d'exécution 42
Afficher la configuration 42
Effacer et supprimer les paramètres de configuration 42

Créer des fichiers de configuration texte hors ligne 44
Appliquer les modifications de configuration aux connexions 45
Recharger l'ASA 45

CHAPITRE 3 **Licences : licence à clé d'autorisation de produit pour l'ISA 3000** 47
À propos des licences PAK 47
Licence préinstallée 47
Licence permanente 47
Licences à durée limitée 48
Lignes directrices relatives à l'activation de la licence à durée limitée 48
Fonctionnement de la minuterie des licences à durée limitée 48
Association des licences permanentes et à durée limitée 48
Empilage des licences à durée limitée 49
Échéance de la licence à durée limitée 50
Remarques relatives à la licence 50
LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement 50
Autre licence VPN 50
Nombre total de sessions VPN combinées, tous types 51
Équilibrage de la charge VPN 51
Licences VPN existantes 51
Licence de chiffrement 51
Nombre total de sessions de mandataire TLS 51
Nombre maximum de VLAN 52
Licences partagées Secure Client (services client sécurisés) Premium (AnyConnect 3 et versions antérieures) 53
Licences de basculement 53
Exigences et exceptions en matière de licence de basculement 53
Association des licences de basculement 53
Perte de communication entre les unités de basculement 54
Mise à niveau des paires de basculement 54
Aucun modèle de chiffrement des données utiles 54
FAQ sur les licences 55
Lignes directrices relatives aux licences PAK 56
Configurer les licences PAK 57

Commander des licences PAK et obtenir une clé d'activation 57
Obtenir une licence de cryptage renforcé 59
Activer ou désactiver les clés 61
Configurer une licence partagée (Secure Client (services client sécurisés) 3 et versions antérieures) 62
À propos des licences partagées 62
À propos du serveur de licences partagées et des participants 62
Problèmes de communication entre le participant et le serveur 64
À propos du serveur de sauvegarde de licences partagées 64
Licences de basculement et partagées 65
Nombre maximum de participants 66
Configurer le serveur de licences partagées 67
Configurer le serveur de sauvegarde de licences partagées (facultatif) 68
Configurer le participant à la licence partagée 69
Licences de fonctionnalités prises en charge par modèle 70
Licences par modèle 70
Fonctionnalités de la licence ISA 3000 70
Supervision des licences PAK 71
Affichage de votre licence actuelle 71
Supervision de la licence partagée 80
Historique des licences PAK 81

CHAPITRE 4 **Licences : gestion des licences logicielles Smart 89**
À propos des licences logicielles Smart 89
Licences logicielles Smart pour l'ASA sur le Châssis Firepower 4100/9300 90
Gestionnaire de logiciels et comptes Smart 90
Gestion hors ligne 91
Réservation de licence permanente 91
Smart Software Manager sur place 95
Licences et appareils gérés par compte virtuel 95
Licence d'évaluation. 95
À propos des licences par type 96
LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement 97
Autres homologues VPN 97
Total des homologues VPN combinés, tous types 97

Licence de chiffrement 97
Licence d'opérateur 100
Nombre total de sessions de mandataire TLS 100
Nombre maximum de VLAN 101
Licence de filtre de trafic de réseau de zombies 101
Licences de basculement ou de grappe ASA 101
Licences de basculement pour l'ASAv 101
Licences de basculement pour Firepower 1010 102
Licences de basculement pour Firepower 1100 102
Licences de basculement pour Firepower 2100 104
Licences de basculement pour Cisco Secure Firewall 3100 105
Licences de basculement pour l'Firepower 4100/9300 107
Licences de grappe ASA pour Cisco Secure Firewall 3100 108
Licences de grappe ASA pour l'ASAv 109
Licences de grappe ASA pour l'Firepower 4100/9300 110
Conditions préalables à la gestion de licences logicielles Smart 111
Conditions préalables de Smart Software Manager standard et sur site 111
Conditions préalables à la réservation de licence permanente 112
Gestion des licences logicielles Smart 112
Paramètres par défaut des licences logicielles Smart 113
ASA virtuel : configurer les licences logicielles Smart 113
ASA virtuel : configurer les licences logicielles Smart standard 113
ASA virtuel : configurer les licences Smart Software Manager sur site 118
ASA virtuel: configurer les licences logicielles Smart Utility (MSLA) 122
ASA virtuel: configurer la réservation de licence permanente 128
Installer la licence permanente ASA virtuel 128
(Facultatif) Retourner la licence permanente ASA virtuel 131
(Facultatif) Annuler l'enregistrement de l'ASA virtuel (standard et sur site) 132
(Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASA virtuel (standard et sur site) 132
1000/2100/3100 : configurer les licences logicielles Smart 133
1000/2100/3100 : configurer les licences logicielles Smart standard 133
1000/2100/3100 : configurer les licences Smart Software Manager sur site 138
1000/2100/3100 : configurer la réservation de licence permanente 141

Installer la licence permanente 1000/2100/3100 141
(Facultatif) Renvoyez la licence permanente 1000/2100/3100 144
(Facultatif) Annuler l'enregistrement de 1000/2100/3100 (standard et sur site) 145
(Facultatif) Renouveler le certificat d'ID ou le droit de licence des modèles 1000/2100/3100 (standard et sur site) 146
Firepower 4100/9300 : configurer les licences logicielles Smart 146
Licences par modèle 149
ASA virtuel 149
Firepower 1010 154
Gamme Firepower 1100 155
Firepower Série 2100 157
Gamme Secure Firewall 3100 158
Firepower 4100 159
Firepower 9300 161
PID de licence par modèle 161
Supervision des licences logicielles Smart 165
Affichage de votre licence actuelle 165
Affichage de l'état de la licence Smart 166
Affichage de l'UDI 169
Débogage des licences logicielles Smart 169
Communication avec Smart Software Manager 169
Enregistrement de l'appareil et jetons 169
Communication périodique avec le Smart Software Manager 170
État de non-conformité 170
Infrastructure Smart Call Home 171
Gestion des certificats de licence Smart 171
Historique des licences logicielles Smart 171

CHAPITRE 5 **Périphériques logiques pour le Firepower 4100/9300** 175
À propos des interfaces 175
Interface de gestion de châssis 175
Types d'interface 176
Interfaces FXOS par rapport aux interfaces d'application 177
À propos des périphériques logiques 178

Périphériques logiques autonomes et en grappe 178
Exigences et conditions préalables pour les combinaisons matérielles et logicielles 179
Lignes directrices et limites relatives aux périphériques logiques 180
Lignes directrices et limites des interfaces 180
Lignes directrices et limites générales 180
Exigences et prérequis pour la haute accessibilité 181
Interfaces de configuration 181
Configurer une interface physique 181
Ajouter un canal EtherChannel (canal de port) 183
Configurer les périphériques logiques 186
Ajouter un ASA autonome 186
Ajouter une paire à haute disponibilité 192
Modifier une interface sur un périphérique logique ASA 193
Se connecter à la console de l'application 194
Historique des périphériques logiques 196

CHAPITRE 6 **Mode pare-feu transparent ou routé 199**
À propos du mode pare-feu 199
À propos du mode de pare-feu routé 199
À propos du mode de pare-feu transparent 199
Utilisation du pare-feu transparent au sein de votre réseau 200
Interface Management (gestion) 200
Trafic de transfert pour les fonctionnalités en mode routé 200
À propos des groupes de ponts 201
Interface BVI (Bridge Virtual Interface) 201
Groupes de ponts en mode pare-feu transparent 201
Groupes de ponts en mode pare-feu routé 202
Transmission du trafic non autorisée en mode routé 203
Autorisation du trafic de couche 3 203
Adresses MAC autorisées 204
BPDU Handling (gestion des paquets BPDU) 204
Recherches d'adresse MAC ou de route 204
Fonctionnalités non prises en charge pour les groupes de ponts en mode transparent 206
Fonctionnalités non prises en charge pour les groupes de ponts en mode routé 207

Paramètres d'usine 208
Lignes directrices sur le mode pare-feu 208
Définir le mode du pare-feu 210
Exemples de mode de pare-feu 211
Progression des données dans l'ASA en mode de pare-feu routé 211
Un utilisateur interne visite un serveur web 211
Un utilisateur externe visite un serveur web sur la DMZ 212
Un utilisateur interne visite un serveur web sur la DMZ 213
Un utilisateur externe tente d'accéder à un hôte interne 214
Un utilisateur DMZ tente d'accéder à un hôte interne 215
Progression des données dans le pare-feu transparent 215
Un utilisateur interne visite un serveur web 216
Un utilisateur interne visite un serveur web à l'aide de la NAT 217
Un utilisateur externe visite un serveur web sur le réseau interne 219
Un utilisateur externe tente d'accéder à un hôte interne 220
Historique du mode de pare-feu 221

PARTIE II **Fonctionnalités de haute disponibilité et d'évolutivité** 223

CHAPITRE 7 **Mode contexte multiple** 225
À propos des contextes de sécurité 225
Utilisations courantes des contextes de sécurité 225
Fichiers de configuration de contexte 226
Configurations de contexte 226
Configuration système 226
Configuration du contexte d'administration 226
Classement des paquets par l'ASA 226
Critères de classificateurs valides 226
Exemples de classement 227
Contextes de sécurité en cascade 230
Accès de gestion aux contextes de sécurité 231
Accès à l'administrateur système 231
Accès à l'administrateur de contexte 231
Utilisation de l'interface de gestion 231

À propos de la gestion des ressources 232
Classes des ressources 232
Limites des ressources 232
Classe par défaut 233
Utiliser des ressources surexploitées 234
Utiliser des ressources illimitées 234
À propos des adresses MAC 235
Adresses MAC en mode de contexte multiple 235
Adresses MAC automatiques 235
Prise en charge du VPN 236
Licences pour le mode de contexte multiple 237
Conditions préalables pour le mode de contexte multiple 238
Lignes directrices pour le mode de contexte multiple 238
Paramètres par défaut du mode de contexte multiple 239
Configurer plusieurs contextes 239
Activer ou désactiver le mode de contexte multiple 240
Activer le mode de contexte multiple 240
Rétablir le mode de contexte unique 241
Configurer une classe pour la gestion des ressources 242
Configurer un contexte de sécurité 246
Attribuer automatiquement des adresses MAC aux interfaces de contexte 250
Changer entre les contextes et l'espace d'exécution du système 251
Gérer les contextes de sécurité 252
Supprimer un contexte de sécurité 252
Modifier le contexte d'administration 252
Modifier l'URL du contexte de sécurité 253
Recharger un contexte de sécurité 254
Recharger en effaçant la configuration 255
Recharger en supprimant et en rajoutant le contexte 255
Supervision des contextes de sécurité 256
Afficher les informations de contexte 256
Afficher l'affectation des ressources 257
Afficher l'utilisation des ressources 260
Superviser les attaques SYN dans les contextes 263

Afficher les adresses MAC attribuées 265
Afficher les adresses MAC dans la configuration système 265
Afficher les adresses MAC dans un contexte 266
Exemples de mode de contexte multiple 267
Historique du mode de contexte multiple 268

CHAPITRE 8 **Basculement pour la haute disponibilité 273**
À propos du basculement 273
Modes de basculement 273
Configuration système requise pour Failover (basculement) 274
Configuration matérielle requise 274
Configuration logicielle requise 274
Exigences de licence 275
Liens de basculement et de basculement avec état 275
Lien de basculement 275
Lien de basculement dynamique 277
Éviter le basculement interrompu et les liaisons de données 278
Les adresses MAC et les adresses IP en Failover (basculement) 279
Basculement avec et sans état 281
Basculement sans état 281
Basculement avec état 282
Exigences en matière de groupes de ponts pour le basculement 284
Exigences en matière de groupes de ponts pour les appareils, ASAv 284
Surveillance de l'intégrité du basculement 284
Surveillance de l'intégrité de l'unité 284
Surveillance d'interfaces 285
détection 286
Synchronisation de la configuration 288
Réplication de la configuration en cours d'exécution 288
Réplication du fichier 288
Réplication de la commande 289
Optimisation de la synchronisation et de la configuration 290
À propos du basculement actif/de secours 291
Rôles principal/secondaire et état actif/de secours 291

Détermination de l'unité active au démarrage 291
Événements de basculement 291
À propos du basculement actif/actif 292
Présentation du basculement actif/actif 293
Rôles principal/secondaire et état actif/de secours pour un groupe de basculement 293
Détermination de l'unité active pour les groupes de basculement au démarrage 293
Événements de basculement 294
Licences pour le basculement 295
Lignes directrices pour Failover (basculement) 296
Paramètres par défaut pour le basculement 299
Configurer le basculement actif/de secours 299
Configurer l'unité principale pour le basculement actif/de secours 300
Configurer l'unité secondaire pour le basculement actif/de secours 303
Configurer le basculement actif/actif 304
Configurer l'unité principale pour le basculement actif/actif 304
Configurer l'unité secondaire pour le basculement actif/actif 309
Configurer les paramètres de basculement facultatifs 310
Configurer les critères de basculement et les autres paramètres 310
Configurer la supervision de l'interface 315
Configurer la prise en charge des paquets routés asymétriques (mode actif/actif) 315
Gérer Failover (basculement) 319
Forcer le basculement 319
Désactiver le basculement 320
Restaurer une unité défaillante 321
Resynchroniser la configuration 322
Tester la fonctionnalité de basculement 322
Exécution de la commande à distance 323
Envoyer une commande 323
Modifier les modes de commande 323
Questions de sécurité 324
Limites de l'exécution de la commande à distance 325
Surveillance de Failover (basculement) 325
Messages de basculement 325
Messages de journal système de basculement 325

Messages de débogage de basculement 326
Interruptions de basculement SNMP 326
Supervision de l'état du basculement 326
Historique de basculement 326

CHAPITRE 9 **Basculement pour la haute disponibilité dans le nuage public 331**
À propos du basculement dans le nuage public 331
À propos du basculement actif/de secours 332
Rôles principal/secondaire et état actif/de secours 332
Connexion de basculement 332
Messages de sondage et Hello 333
Détermination de l'unité active au démarrage 333
Événements de basculement 333
Lignes directrices et limites relatives à la licence 335
Licences pour le basculement dans le nuage public 336
Valeurs par défaut pour le basculement dans le nuage public 336
À propos de l'ASA virtuel à haute disponibilité dans Microsoft Azure 337
À propos du principal de service Azure 338
Exigences de configuration pour ASA virtuel haute disponibilité dans Azure 339
Configurer le basculement actif/de secours 340
Configurer l'unité principale pour le basculement actif/de secours 340
Configurer l'unité secondaire pour le basculement actif/de secours 341
Configurer les paramètres de basculement facultatifs 342
Configurer les critères de basculement et les autres paramètres 342
Configurer les informations d'authentification pour un principal de service Azure 344
Configurer les tableaux de routage Azure 345
Activer le basculement actif/de secours 347
Activer l'unité principale pour le basculement actif/de secours 347
Activer l'unité secondaire pour le basculement actif/de secours 348
Gérer le basculement dans le nuage public 349
Forcer le basculement 349
Mettre à jour les routes 349
Valider l'authentification Azure 350
Superviser le basculement dans le nuage public 351

État de basculement 351
Messages de basculement 351
Historique de basculement dans le nuage public 352

CHAPITRE 10 **Grappe ASA pour le Secure Firewall 3100** 353
À propos de la mise en grappe d'ASA 353
Intégration de la grappe dans votre réseau 353
Membres de la grappe 354
Configuration du démarrage 354
Rôles des nœuds de contrôle et de données 354
Interfaces de la grappe 354
Liaison de commande de grappe 354
Réplication de la configuration 355
Gestion de la grappe ASA 355
Réseau de gestion 355
Interface de gestion 355
Gestion de l'unité de contrôle vs Gestion de l'unité de données 356
duplication de clé de chiffrement 356
Incompatibilité d'adresse IP du certificat de connexion ASDM 356
Mise en grappe inter-sites 356
Licences pour la mise en grappe d'ASA 357
Exigences et conditions préalables à la mise en grappe ASA 358
Lignes directrices de la mise en grappe 360
Configurer la mise en grappe ASA 365
Câbler les unités et configurer les interfaces 366
À propos des interfaces de grappe 366
Câbler les unités de grappe et configurer les équipements en amont et en aval 370
Configurer le mode d'interface de grappe de chaque unité 371
Configurer les interfaces sur le nœud de contrôle 372
Créer la configuration de démarrage 378
Configurer les paramètres de démarrage du nœud de contrôle 378
Configurer les paramètres de démarrage du nœud de données 383
Personnaliser l'opération de mise en grappe 385
Configurer les paramètres de grappe ASA de base 385

Configurer les paramètres de surveillance de l'intégrité et de jonction automatique 386
Configurer la rééquilibrage de la connexion et le délai de réplication TCP de la grappe 390
Configurer les fonctionnalités inter-sites 391
Gérer les nœuds de la grappe 398
Devenir un nœud inactif 398
Désactiver undonnées 399
Rejoindre la grappe 399
Quitter la grappe 400
Modifier le nœud de contrôle 401
Exécuter une commande à l'échelle de la grappe 402
Supervision de la grappe ASA 403
Supervision de l'état de la grappe 403
Capture des paquets à l'échelle de la grappe 407
Supervision des ressources de la grappe 407
Supervision du trafic de la grappe 408
Supervision du routage de la grappe 413
Configuration de la journalisation pour la mise en grappe 413
Supervision des interfaces de grappe 413
Débogage de la mise en grappe 414
Exemples de mise en grappe ASA 415
Exemple de configuration ASA et du commutateur 415
Configuration ASA 415
Configuration du commutateur Cisco IOS 417
Pare-feu sur clé 418
Ségrégation du trafic 420
Configuration OTV pour la mise en grappe inter-sites en mode routé 422
Exemples de mise en grappe inter-sites 425
Exemple de mode de routage EtherChannel étendu avec des adresses MAC et IP propres au site 425
Exemple intersites nord-sud de mode transparent de l'EtherChannel étendu 426
Exemple inter-sites est-ouest en mode transparent de l'EtherChannel étendu 427
Référence pour la mise en grappe 428
Fonctionnalités et mise en grappe de l'ASA 428
Fonctionnalités non prises en charge par la mise en grappe 429
Fonctionnalités centralisées pour la mise en grappe 429

Fonctionnalités appliquées aux nœuds individuels 430
AAA pour l'accès réseau et la mise en grappe 431
Paramètres de connexion et mise en grappe 431
FTP et mise en grappe 431
Inspection ICMP et mise en grappe 432
Routage multidiffusion et mise en grappe 432
NAT et mise en grappe 432
Routage et mise en grappe dynamiques 434
SCTP et mise en grappe 435
Inspection SIP et mise en grappe 435
SNMP et mise en grappe 435
STUN et mise en grappe 435
Syslog, NetFlow et la mise en grappe 435
Cisco TrustSec et la mise en grappe 436
VPN et mise en grappe 436
Facteur d'évolutivité de rendement 436
Choix du nœud de contrôle 436
Haute disponibilité au sein de la grappe 437
Surveillance de l'intégrité du nœud 437
Surveillance d'interfaces 437
État après l'échec 438
Rejoindre la grappe 438
Réplication de l'état de la connexion du chemin de données 439
Gestion des connexions par la grappe 439
Rôles de connexion 439
Nouvelle propriété de connexion 442
Exemple de flux de données pour TCP 442
Exemple de flux de données pour ICMP et UDP 443
Rééquilibrage des nouvelles connexions TCP dans la grappe 444
Historique de la mise en grappe d'ASA pour le Secure Firewall 444

CHAPITRE 11 **Grappe ASA pour le Firepower 4100/9300** 445
À propos de la mise en grappe sur les châssis Firepower 4100/9300 445
Configuration du démarrage 446

Membres de la grappe 446
Liaison de commande de grappe 446
Dimensionner la liaison de commande de grappe 447
Redondance de la liaison de commande de la grappe 448
Fiabilité de la liaison de commande de grappe pour la mise en grappe 448
Réseau de liaison de commande de grappe 448
Interfaces de la grappe 448
Connexion à un système de commutateurs redondants 449
Réplication de la configuration 449
Gestion des grappes Cisco Secure Firewall ASA 449
Réseau de gestion 449
Interface de gestion 449
Gestion de l'unité de contrôle vs Gestion de l'unité de données 450
duplication de clé de chiffrement 450
Incompatibilité d'adresse IP du certificat de connexion ASDM 450
EtherChannels étendus (recommandé) 450
Mise en grappe inter-sites 451
Exigences et conditions préalables à la mise en grappe sur Châssis Firepower 4100/9300 452
Licences pour la mise en grappe sur le Châssis Firepower 4100/9300 454
Lignes directrices et limites de la mise en grappe 455
Configurer la mise en grappe sur le Châssis Firepower 4100/9300 460
FXOS : Ajouter une grappe ASA 461
Créer une grappe ASA 461
Ajouter d'autres membres à la grappe 471
ASA : Modifier le mode de pare-feu et le mode de contexte 471
ASA : Configurer les interfaces de données 472
ASA : Personnaliser la configuration de la grappe 475
Configurer les paramètres de grappe ASA de base 475
Configurer les paramètres de surveillance de l'intégrité et de jonction automatique 477
Configurer la rééquilibrage de la connexion et le délai de réplication TCP de la grappe 481
Configurer les fonctionnalités inter-sites 482
Configurer le VPN de site à site distribué 489
FXOS : supprimer un nœud de la grappe 495
ASA : Gérer les membres de la grappe 497

Devenir un membre inactif 497
Désactiver une données 498
Rejoindre la grappe 499
Changer l'unité de contrôle 500
Exécuter une commande à l'échelle de la grappe 500
ASA : supervision de la grappe ASA sur le Châssis Firepower 4100/9300 501
Supervision de l'état de la grappe 502
Capture des paquets à l'échelle de la grappe 506
Supervision des ressources de la grappe 506
Supervision du trafic de la grappe 506
Supervision du routage de la grappe 510
Supervision du VPN S2S distribué 511
Configuration de la journalisation pour la mise en grappe 511
Débogage de la mise en grappe 512
Dépannage du VPN S2S distribué 512
Exemples de mise en grappe d'ASA 514
Pare-feu sur clé 514
Ségrégation du trafic 515
Configuration OTV pour la mise en grappe inter-sites en mode routé 515
Exemples de mise en grappe inter-sites 518
Exemple de mode de routage EtherChannel étendu avec des adresses MAC et IP propres au site 518
Exemple intersites nord-sud de mode transparent de l'EtherChannel étendu 519
Exemple inter-sites est-ouest en mode transparent de l'EtherChannel étendu 521
Référence pour la mise en grappe 522
Fonctionnalités et mise en grappe de l'ASA 522
Fonctionnalités non prises en charge par la mise en grappe 522
Fonctionnalités centralisées pour la mise en grappe 523
Fonctionnalités appliquées aux unités individuelles 524
AAA pour l'accès réseau et la mise en grappe 525
Paramètres de connexion 525
FTP et mise en grappe 525
Inspection ICMP 525
Routage multidiffusion et mise en grappe 525
NAT et mise en grappe 525

Routage et mise en grappe dynamiques 527
SCTP et mise en grappe 528
Inspection SIP et mise en grappe 528
SNMP et mise en grappe 528
STUN et mise en grappe 529
Syslog, NetFlow et la mise en grappe 529
Cisco TrustSec et la mise en grappe 529
VPN et mise en grappe sur le châssis Cisco Secure Firewall eXtensible Operating System (FXOS) 529
Facteur d'évolutivité de rendement 530
Choix d'unité de contrôle 530
Haute disponibilité au sein de la grappe 531
Surveillance des applications du châssis 531
Surveillance de l'intégrité de l'unité 531
Surveillance d'interfaces 531
Surveillance de l'application Decorator 532
État après l'échec 532
Rejoindre la grappe 532
Réplication de l'état de la connexion du chemin de données 533
Gestion des connexions par la grappe 533
Rôles de connexion 533
Nouvelle propriété de connexion 536
Exemple de flux de données pour TCP 536
Exemple de flux de données pour ICMP et UDP 537
Rééquilibrage des nouvelles connexions TCP dans la grappe 538
Historique de la mise en grappe d'ASA sur le Firepower 4100/9300 538

CHAPITRE 12 **Grappe ASA pour l'ASA virtuel pour le cloud privé 545**
À propos de la mise en grappe d'ASA virtuel 546
Intégration de la grappe dans votre réseau 546
Nœuds de la grappe 546
Configuration du démarrage 546
Rôles des nœuds de contrôle et de données 546
Interfaces individuelles 547

Routage à base de règles 548
Routage à chemins multiples à coût égal 548
Liaison de commande de grappe 548
Présentation du trafic de liaison de commande de grappe 549
Échec de la liaison de commande de grappe 549
Réplication de la configuration 550
Gestion des grappes ASA virtuel 550
Réseau de gestion 550
Interface de gestion 550
Gestion de nœud de contrôle vs Gestion de nœud de données 550
duplication de clé de chiffrement 551
Incompatibilité d'adresse IP du certificat de connexion ASDM 551
Mise en grappe inter-sites 551
Licences pour la mise en grappe d'ASA virtuel 552
Exigences et conditions préalables à la mise en grappe d'ASA virtuel 552
Lignes directrices de la mise en grappe d'ASA virtuel 553
Configurer la mise en grappe d'ASA virtuel à l'aide d'une configuration Day0 554
Configurer la mise en grappe ASA virtuel après le déploiement 557
Configurer les paramètres d'interface 557
Configurer le mode d'interface de grappe de chaque nœud 557
Configurer les interfaces individuelles 558
Créer la configuration de démarrage 561
Configurer les paramètres de démarrage du nœud de contrôle 561
Configurer les paramètres de démarrage du nœud de données 567
Personnaliser l'opération de mise en grappe 570
Configurer les paramètres de grappe ASA de base 570
Configurer les paramètres de surveillance de l'intégrité et de jonction automatique 571
Configurer la rééquilibrage de la connexion et le délai de réplication TCP de la grappe 574
Configurer les fonctionnalités inter-sites 575
Activer la localisation du directeur 575
Activer la redondance de site 576
Configurer la mobilité des flux de grappes 576
Gérer les nœuds de la grappe 581
Devenir un nœud inactif 581

Désactiver un nœud de données à partir du nœud de contrôle 582
Rejoindre la grappe 583
Quitter la grappe 583
Modifier le nœud de contrôle 584
Exécuter une commande à l'échelle de la grappe 585
Supervision de la grappe ASA virtuel 586
Supervision de l'état de la grappe 586
Capture des paquets à l'échelle de la grappe 590
Supervision des ressources de la grappe 590
Supervision du trafic de la grappe 590
Supervision du routage de la grappe 595
Configuration de la journalisation pour la mise en grappe 596
Supervision des interfaces de grappe 596
Débogage de la mise en grappe 596
Exemples de mise en grappe d'ASA virtuel 597
Exemple inter-sites nord-sud de mode routé d'interface individuelle 597
Référence pour la mise en grappe 598
Fonctionnalités et mise en grappe de l'ASA 598
Fonctionnalités non prises en charge par la mise en grappe 598
Fonctionnalités centralisées pour la mise en grappe 599
Fonctionnalités appliquées aux nœuds individuels 600
AAA pour l'accès réseau et la mise en grappe 600
Paramètres de connexion et mise en grappe 601
Routage et mise en grappe dynamiques 601
FTP et mise en grappe 602
Inspection ICMP et mise en grappe 602
Routage multidiffusion et mise en grappe 602
NAT et mise en grappe 602
SCTP et mise en grappe 604
Inspection SIP et mise en grappe 604
SNMP et mise en grappe 605
STUN et mise en grappe 605
Syslog, NetFlow et la mise en grappe 605
Cisco TrustSec et la mise en grappe 605

VPN et mise en grappe 605
Facteur d'évolutivité de rendement 606
Choix du nœud de contrôle 606
Haute disponibilité au sein de la grappe ASA virtuel 607
Surveillance de l'intégrité du nœud 607
Surveillance d'interfaces 607
État après l'échec 607
Rejoindre la grappe 608
Réplication de l'état de la connexion du chemin de données 608
Gestion des connexions par la grappe ASA virtuel 609
Rôles de connexion 609
Nouvelle propriété de connexion 611
Exemple de flux de données pour TCP 611
Exemple de flux de données pour ICMP et UDP 612
Rééquilibrage des nouvelles connexions TCP dans la grappe 613
Historique de la mise en grappe d'ASA virtuel 614

CHAPITRE 13 **Grappe ASA pour l'ASA virtuel dans un nuage public** 615
À propos de la mise en grappe d'ASA virtuel dans le nuage public 615
Intégration de la grappe dans votre réseau 616
Nœuds de la grappe 616
Configuration du démarrage 616
Rôles des nœuds de contrôle et de données 617
Interfaces individuelles 617
Liaison de commande de grappe 617
Présentation du trafic de liaison de commande de grappe 618
Échec de la liaison de commande de grappe 618
Réplication de la configuration 618
Gestion des grappes ASA virtuel 619
Réseau de gestion 619
Interface de gestion 619
Gestion de nœud de contrôle vs Gestion de nœud de données 619
duplication de clé de chiffrement 620
Incompatibilité d'adresse IP du certificat de connexion ASDM 620

Licences pour la mise en grappe d'ASA virtuel 620
Exigences et conditions préalables à la mise en grappe d'ASA virtuel 620
Lignes directrices relatives à la mise en grappe d'ASA virtuel 622
Déployer la grappe dans AWS 623
Équilibreur de charge de passerelle AWS et serveur mandataire à un seul volet de Geneve 623
Exemple de topologie 624
Processus de bout en bout pour le déploiement de la grappe ASA virtuel sur AWS 625
Modèles 626
Déployer la pile dans AWS à l'aide d'un modèle CloudFormation 626
Déployer manuellement la grappe dans AWS 630
Créer la configuration Day0 pour AWS 630
Déployer les nœuds de la grappe 632
Personnaliser l'opération de mise en grappe 633
Configurer les paramètres de grappe ASA de base 633
Configurer les paramètres de surveillance de l'intégrité et de jonction automatique 634
Gérer les nœuds de la grappe 637
Devenir un nœud inactif 637
Désactiver un nœud de données à partir du nœud de contrôle 637
Rejoindre la grappe 638
Quitter la grappe 639
Modifier le nœud de contrôle 640
Exécuter une commande à l'échelle de la grappe 640
Surveillance de la grappe 641
Supervision de l'état de la grappe 641
Capture des paquets à l'échelle de la grappe 645
Supervision des ressources de la grappe 645
Supervision du trafic de la grappe 646
Supervision du routage de la grappe 651
Configuration de la journalisation pour la mise en grappe 651
Supervision des interfaces de grappe 651
Débogage de la mise en grappe 652
Référence pour la mise en grappe 652
Fonctionnalités et mise en grappe de l'ASA 653
Fonctionnalités non prises en charge par la mise en grappe 653

Fonctionnalités centralisées pour la mise en grappe 653
Fonctionnalités appliquées aux nœuds individuels 654
AAA pour l'accès réseau et la mise en grappe 655
Paramètres de connexion et mise en grappe 655
Routage et mise en grappe dynamiques 655
FTP et mise en grappe 656
Inspection ICMP et mise en grappe 657
Routage multidiffusion et mise en grappe 657
NAT et mise en grappe 657
SCTP et mise en grappe 659
Inspection SIP et mise en grappe 659
SNMP et mise en grappe 659
STUN et mise en grappe 659
Syslog et mise en grappe 660
Cisco Trustsec et mise en grappe 660
VPN et mise en grappe 660
Facteur d'évolutivité de rendement 660
Choix du nœud de contrôle 660
Haute disponibilité au sein de la grappe 661
Surveillance de l'intégrité du nœud 661
Surveillance d'interfaces 662
État après l'échec 662
Rejoindre la grappe 662
Réplication de l'état de la connexion du chemin de données 663
Gestion des connexions par la grappe 663
Rôles de connexion 663
Nouvelle propriété de connexion 666
Exemple de flux de données pour TCP 666
Exemple de flux de données pour ICMP et UDP 667
Historique de la mise en grappe d'ASA virtuel dans le nuage public 668

PARTIE III **Interfaces** 669

CHAPITRE 14 **Configuration de l'interface de base** 671

À propos de la configuration de l'interface de base 671
Fonctionnalité Auto-MDI/MDIX 671
Interface de gestion 672
Présentation de l'interface de gestion 672
L'interface de logement/port de gestion 672
Utiliser n'importe quelle interface pour le trafic de gestion uniquement 673
Interface de gestion pour le mode transparent 673
Lignes directrices pour la configuration de l'interface de base 674
Paramètres par défaut pour la configuration de l'interface de base 674
Activer l'interface physique et configurer les paramètres Ethernet 675
Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000) 678
Gérer le module de réseau pour Cisco Secure Firewall 679
Configurer les ports d'éclatement 680
Ajouter un module de réseau 681
Échange à chaud du module de réseau 681
Remplacer le module de réseau par un module de type différent 682
Retirer le module de réseau 683
Surveillance des interfaces 684
Exemples d'interfaces de base 684
Exemple de paramètres d'interface physique 684
Exemple de mode de contexte multiple 685
Historique de la configuration de l'interface de base 685

CHAPITRE 15 **Configuration de base de l'interface pour les ports de commutation du Firepower 1010** 689
À propos des ports de commutation 689
Comprendre les ports et les interfaces de commutation 689
Fonctionnalité Auto-MDI/MDIX 690
Lignes directrices et limites pour les ports de commutation 690
Configurer les ports de commutation et l'alimentation par Ethernet (PoE) 692
Activer ou désactiver le mode Port de commutation 692
Configurer une interface VLAN 693
Configurer les ports de commutation comme ports d'accès 694
Configurer les ports de commutation comme ports de ligne principale 696
Configurer Power Over Ethernet (alimentation électrique par câble Ethernet) 699

Supervision des ports de commutation 700
Exemples de ports de commutation 701
Exemple de mode routé 701
Exemple de mode transparent 702
Exemple d'interface de pare-feu/port de commutation mixte 702
Exemple de routage et pont intégrés 703
Exemple de basculement 704
Historique des ports de commutation 705

CHAPITRE 16 **Interfaces EtherChannel 707**
À propos des EtherChannels 707
About EtherChannels 707
Interfaces des groupes de canaux 708
Connexion à un EtherChannel sur un autre périphérique 708
Protocole LACP (Link Aggregation Control Protocol) 709
Équilibrage de la charge 709
Adresse MAC de l'EtherChannel 710
Directives pour les EtherChannels 710
Paramètres par défaut pour les interfaces EtherChannels 712
Configurer un EtherChannel 713
Ajouter des interfaces à l'EthernetChannel 713
Personnaliser l'EtherChannel (ISA 3000) 715
Supervision des EtherChannels 717
Exemples d'EtherChannels 718
Historique des EtherChannels 718

CHAPITRE 17 **Interfaces de boucle avec retour 721**
À propos des interfaces de boucle avec retour 721
Directives pour les interfaces de boucle avec retour 722
Configurer une interface de boucle avec retour 722
Limite de débit du trafic vers l'interface de boucle avec retour 722
Supervision des interfaces de boucle avec retour 724
Historique des interfaces de boucle avec retour 724

CHAPITRE 18 **Sous-interfaces VLAN** 727

À propos des sous-interfaces VLAN 727

Licences pour les sous-interfaces VLAN 727

Lignes directrices et limites pour les sous-interfaces VLAN 728

Paramètres par défaut pour les sous-interfaces VLAN 729

Configurer les sous-interfaces VLAN et la jonction 802.1Q 729

Supervision des sous-interfaces VLAN 731

Exemples de sous-interfaces VLAN 731

Historique des sous-interfaces VLAN 732

CHAPITRE 19 **Interfaces VXLAN** 735

À propos des interfaces VXLAN 735

Encapsulation 735

Point terminal du tunnel VXLAN 736

Interface de la source VTEP 736

Interface VNIs 737

Traitement de paquet VXLAN 737

Pair VTEP 738

Scénarios VXLAN 739

Présentation du pont ou de la passerelle VXLAN 739

Pont VXLAN 739

Passerelle VXLAN (mode routé) 740

Routeur entre domaines VXLAN 740

Équilibreur de charge de passerelle AWS et serveur mandataire à un seul volet de Geneve 741

Équilibreur de charge de passerelle Azure et serveur mandataire jumelé 742

Exigences et conditions préalables pour les interfaces VXLAN 743

Lignes directrices pour les interfaces VXLAN 743

Paramètres par défaut des interfaces VXLAN 744

Configurer les interfaces VXLAN 745

Configurer l'interface source VTEP 745

Configurer l'interface VNI 747

(Facultatif) Modifier le port UDP VXLAN 750

Configurer les interfaces Geneve 750

Configurer l'interface source VTEP pour Geneve 751
Configurer l'interface VNI pour Geneve 752
Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle 753
Supervision des interfaces VXLAN 755
Exemples d'interfaces VXLAN 757
Exemple de passerelle VXLAN transparente 757
Exemple de routage VXLAN 759
Historique des interfaces VXLAN 761

CHAPITRE 20 **Interfaces en mode routage et en mode transparent 763**
À propos des interfaces en mode routage et en mode transparent 763
Niveaux de sécurité 763
Double pile IP (IPv4 et IPv6) 764
Masque de sous-réseau 31 bits 764
Sous-réseau 31 bits et mise en grappe 764
Sous-réseau 31 bits et basculement 765
Gestion et sous-réseau 31 bits 765
Fonctionnalités 31 bits non prises en charge 765
Directives et limites pour les interfaces en mode routé et en mode transparent 765
Configurer les interfaces en mode routé 767
Configurer les paramètres généraux de l'interface en mode routé 768
Configurer le protocole PPPoE 771
Configurer les interfaces de groupe de ponts 772
Configurer la BVI (Bridge Virtual Interface) 772
Configurer les paramètres généraux de l'interface de membre du groupe de ponts 774
Configurer une interface de gestion pour le mode transparent 776
Configuration de l'adressage IPv6 778
À propos d'IPv6 778
Adresse IPv6 778
ID d'interface EUI-64 modifiées 779
Configurer le client de délégation de préfixe IPv6 779
À propos de la délégation de préfixe IPv6 779
Activer le client de délégation de préfixe IPv6 781
Configuration d'une adresse globale IPv6 783

Configurer la découverte des voisins IPv6 786
Supervision des interfaces en mode routé et en mode transparent 790
Statistiques et informations sur l'interface 791
Renseignements sur DHCP 791
PPPoE 794
Découverte de voisin IPv6 795
Exemples d'interfaces en mode routé et en mode transparent 796
Exemple de mode transparent avec 2 groupes de ponts 796
Exemple de segment LAN commuté avec 2 groupes de ponts 796
Historique des interfaces en mode routé et en mode transparent 799

CHAPITRE 21 **Configuration avancée de l'interface 803**
À propos des configurations avancées de l'interface 803
À propos des adresses MAC 803
Adresses MAC par défaut 803
Adresses MAC automatiques 804
À propos de la MTU 805
Chemin de découverte de MTU 805
MTU par défaut 805
MTU et fragmentation. 805
MTU et trames grand format 806
À propos de TCP MSS 806
TCP MSS par défaut 806
Paramètre MSS TCP maximal suggéré 807
Communication inter-interface 807
Communication intra-interface (mode de pare-feu routé) 807
Configurer manuellement l'adresse MAC 807
Attribuer automatiquement des adresses MAC 808
Configurer , la et le TCP MSS 809
Autoriser la communication de niveau de sécurité identique 811
Historique de la configuration avancée de l'interface 811

CHAPITRE 22 **Zones de circulation 813**
À propos des zones de trafic 813

Comportement non zoné 813
Pourquoi utiliser des zones? 813
Routage asymétrique 814
Route perdue 814
Équilibrage de la charge 815
Tables de connexion et de routage par zone 816
Routage ECMP 816
Prise en charge ECMP non zonée 816
Prise en charge ECMP zonée 817
Équilibrage de charges des connexions 817
Basculement vers une route dans une autre zone 817
Politique de sécurité basée sur l'interface 817
Services pris en charge pour les zones de trafic 818
Niveaux de sécurité 818
Interface principale et actuelle pour le flux 818
Rejoindre ou quitter une zone 818
Trafic intra-zone 818
Trafic entrant et sortant 819
Chevauchement d'adresses IP dans une zone 819
Conditions préalables aux zones de trafic 819
Lignes directrices relatives aux zones de trafic 821
Configurer une zone de trafic 822
Supervision des zones de trafic 823
Renseignements sur la zone 823
Connexions de zone 824
Routage de zone 824
Exemple de zones de trafic 825
Historique des zones de trafic 828

PARTIE IV **Paramètres de base** 829

CHAPITRE 23 **Paramètres de base** 831
Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet 831
Régler la date et l'heure 834

Définir les dates des fuseaux horaires et de l’heure avancée 834
Définir la date et l’heure à l’aide du serveur NTP 836
Régler la date et l'heure manuellement 838
Configurer le protocole PTP (Precision Time Protocol) (ISA 3000) 839
Configurer la phrase secrète principale 840
Ajouter ou modifier la phrase secrète principale 841
Désactiver la phrase secrète principale 843
Supprimer la phrase secrète principale 844
Configurer des serveurs DNS 844
Configurer le contournement matériel et l’alimentation double (Cisco ISA 3000) 847
Modifier les performances et le comportement ASP (Accelerated Security Path) 849
Choisir un modèle de validation transactionnelle de moteur de règles 849
Activer l’équilibrage de charges ASP 851
Supervision du cache DNS 852
Historique des paramètres de base 852

CHAPITRE 24 **Services DHCP et DDNS 857**
À propos des services DHCP et DDNS 857
À propos du serveur DHCPv4 857
Options de DHCP 857
À propos du serveur sans état DHCPv6 858
À propos de l'agent relais DHCP 858
Prise en charge du serveur relais DHCP sur VTI 858
Lignes directrices pour les services DHCP et DDNS 859
Configurer le serveur DHCP 861
Activer le serveur DHCPv4 861
Configurer les options DHCPv4 avancées 863
Configurer le serveur sans état DHCPv6 865
Configurer les agents de relais DHCP. 867
Configurer l’agent de relais DHCPv4 867
Configurer l’agent de relais DHCPv6 869
Configuration du DNS dynamique 870
Supervision des services DHCP et DDNS 876
Supervision des services DHCP 876

Dépannage du relais DHCP sur VTI 879
Supervision de l'état DDNS 880
Historique des services DHCP et DDNS 881

CHAPITRE 25 **Certificats numériques 885**
À propos des certificats numériques 885
Cryptographie à clé publique 886
Évolutivité des certificats 887
Paires de clés 887
Point de confiance 888
Inscription de certificat 888
Serveur mandataire pour les demandes SCEP 888
Vérification de la révocation 889
Serveurs CA pris en charge 889
CRL 889
OCSP 891
Certificats et coordonnées de connexion de l'utilisateur 892
Informations d'authentification de l'utilisateur 892
Certificats 892
Lignes directrices pour les certificats numériques 893
Configurer les certificats numériques 896
Configurer les paires de clés 896
Configurer les points de confiance 898
Configurer les CRL pour un point de confiance 903
Exporter ou importer une configuration de point de confiance 906
Configurer les règles de mappage des certificats CA 907
Configurer les identités de référence 910
Obtenir des certificats manuellement 912
Obtenir des certificats automatiquement avec SCEP 914
Configurer la prise en charge du serveur mandataire pour les demandes SCEP 915
Comment configurer des types de certificats spécifiques 917
Certificats de l'autorité de certification (CA) 918
Gestion du serveur CA 918
Définir une alerte d'expiration de certificat (pour les certificats d'identité ou CA) 919

Supervision des certificats numériques 920
Historique de gestion des certificats 922

CHAPITRE 26 **Inspection ARP et table des adresses MAC 925**
À propos de l'inspection ARP et de la table des adresses MAC 925
Inspection ARP pour le trafic de groupe de ponts 925
Tableau d'adresses MAC 926
Paramètres d'usine 926
Lignes directrices pour l'inspection ARP et la table d'adresses MAC 927
Configurer l'inspection ARP et les autres paramètres ARP 927
Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP 927
Activer l'inspection ARP 929
Personnaliser la table des adresses MAC pour les groupes de ponts 929
Ajouter une adresse MAC statique pour les groupes de ponts 929
Définir le délai d'expiration de l'adresse MAC 930
Configurer l'apprentissage de l'adresse MAC 930
Supervision de l'inspection ARP et de la table des adresses MAC 931
Historique de l'inspection ARP et de la table des adresses MAC 932

PARTIE V **Routage IP 935**

CHAPITRE 27 **Aperçu du routage 937**
Détermination du chemin 937
Types de routage pris en charge 938
Statique ou dynamique 938
Chemin unique ou chemin multiple 938
Non hiérarchique ou hiérarchique 939
État de lien ou vecteur de distance 939
Protocoles Internet pris en charge pour le routage 939
Table de routage 940
Mode de remplissage de la table de routage 940
Distances administratives pour les routages 941
Sauvegarde des routes dynamiques et statiques flottantes 942
Prise des décisions de transfert 942

Routage dynamique et Failover (basculement) 943
Routage et mise en grappe dynamiques 943
Routage dynamique en mode EtherChannel étendu 943
Routage dynamique en mode d'interface individuelle 944
Routage dynamique en mode de contexte multiple 945
Gestion des ressources de routage 946
Table de routage pour le trafic de gestion 947
Identification de l'interface de gestion 948
Routage à chemins multiples à coûts égaux (ECMP) 948
Désactiver les demandes ARP du mandataire 949
Afficher la table de routage 949
Historique de l'aperçu du routage 950

CHAPITRE 28 **Routages statiques et par défaut 951**
À propos des routages statiques et par défaut 951
Routage par défaut 951
Routes statiques 952
Routage vers l'interface null0 pour abandonner le trafic indésirable 952
Priorités de routage 952
Routages en mode de pare-feu transparent et de groupes de ponts 952
Suivi du routage statique 953
Lignes directrices pour les routages statiques et par défaut 953
Configurer les routes par défaut et statiques 954
Configurer une route par défaut 954
Configurer une route statique 956
Configurer le suivi de route statique 957
Supervision d'une route statique ou par défaut 958
Exemples de routes statiques ou par défaut 959
Historique des routes statiques et par défaut 959

CHAPITRE 29 **Routage basé sur une stratégie 961**
À propos du routage basé sur les politiques 961
Pourquoi utiliser le routage basé sur des politiques? 962
Routage à accès égal et sensible à la source 962

Qualité de service 962
Réduction des coûts 963
Partage de la charge 963
Mise en œuvre de PBR 963
Lignes directrices pour le routage basé sur des politiques 963
Configurer le routage basé sur les politiques 965
Exemples de routage basé sur des politiques 969
Exemples de configuration de carte de routage 969
Exemple de configuration pour PBR 971
Accès Internet direct à l'aide du réseau WAN défini par logiciel 972
Routage basé sur des politiques en action 974
Historique du routage basé sur des politiques 978

CHAPITRE 30 **Cartes de routage 981**
À propos des cartes de routage 981
Clauses d'autorisation et de refus 982
Valeurs de clause de correspondance et de définition 982
Lignes directrices relatives aux cartes de routage 983
Définir une carte de routage 983
Personnaliser une carte de routage 983
Définir une route pour correspondre à une adresse de destination spécifique 984
Configurer les valeurs de mesure pour une action de routage 985
Exemple de cartes de routage 986
Historique des cartes de routage 986

CHAPITRE 31 **Routage par détection de transfert bidirectionnel (BFD) 989**
À propos du routage BFD 989
Mode asynchrone BFD et fonction d'écho 989
Établissement de la session BFD 990
Négociation de la minuterie BFD 991
Détection de défaillance BFD 992
Scénarios de déploiement BFD 992
Directives pour le routage BFD 993
Configurer BFD 993

Créer le modèle BFD 993
Configurer les interfaces BFD 995
Configurer les cartes BFD 997
Supervision BFD 997
Historique du routage BFD 998

CHAPITRE 32 BGP 999
À propos de BGP 999
Quand utiliser BGP 999
Modifications apportées à la table de routage 1000
Sélection du chemin BGP 1001
Chemins multiples BGP 1002
Lignes directrices BGP 1003
Configurer le protocole BGP 1003
Activer BGP 1004
Définir le meilleur chemin pour un processus de routage BGP 1005
Configurer les listes de politiques 1006
Configurer les filtres de chemin AS 1007
Configurer les règles de communauté 1008
Configurer les paramètres de la famille d'adresses IPv4 1009
Configurer les paramètres généraux de la famille IPv4 1009
Configurer les paramètres d'adresse globale de la famille IPv4 1012
Configurer les paramètres de filtrage de la famille IPv4 1013
Configurer les paramètres de voisin BGP de la famille IPv4 1014
Configurer les paramètres réseau IPv4 1020
Configurer les paramètres de redistribution IPv4 1021
Configurer les paramètres d'injection de route IPv4 1022
Configurer les paramètres de la famille d'adresses IPv6 1023
Configurer les paramètres généraux de la famille IPv6 1023
Configurer les paramètres d'adresse globale de la famille IPv6 1024
Configurer les paramètres de voisin BGP de la famille IPv6 1025
Configurer les paramètres réseau IPv6 1031
Configurer les paramètres de redistribution IPv6 1032
Configurer les paramètres d'injection de route IPv6 1034

Supervision BGP 1034
Exemple de BGP 1037
Historique de BGP 1039

CHAPITRE 33 OSPF 1041
À propos d'OSPF 1041
Prise en charge OSPF pour les paquets Fast Hello 1043
Conditions préalables à la prise en charge d'OSPF pour les paquets Fast Hello 1043
À propos de la prise en charge OSPF pour les paquets Hello rapides 1043
Différences d'implémentation entre OSPFv2 et OSPFv3 1044
Directives pour OSPF 1044
Configurer le protocole OSPFv2 1047
Configurer une chaîne de clés pour l'authentification 1048
Configurer l'ID de routeur OSPFv2 1051
Configurer manuellement l'ID de routeur OSPF 1051
Comportement de l'ID de routeur lors de la migration 1052
Configurer les paquets Hello rapides OSPF 1052
Personnaliser le protocole OSPFv2 1053
Redistribuer les routes dans OSPFv2 1053
Configurer la synthèse des routes lors de la redistribution des routes dans OSPFv2 1055
Ajouter une adresse sommaire de route 1055
Configurer la synthèse des routes entre les zones OSPFv2 1056
Configurer les paramètres d'interface OSPFv2 1057
Configurer les paramètres de zone OSPFv2 1060
Configurer les règles de filtre OSPFv2 1061
Configurer une NSSA OSPFv2 1062
Configurer un ensemble d'adresses IP pour la mise en grappe (OSPFv2 et OSPFv3) 1063
Définir les voisins OSPFv2 statiques 1064
Configurer les minuteries de calcul de routage 1065
Journaliser les voisins en hausse ou en baisse 1065
Configurer une chaîne de clés pour l'authentification 1066
Configurer le protocole OSPFv3 1069
Activer OSPFv3 1069
Configurer les paramètres d'interface OSPFv3 1069

Configurer les paramètres de routeur OSPFv3 1075
Configurer les paramètres de zone OSPFv3 1078
Configurer des interfaces passives OSPFv3 1080
Configurer la distance administrative OSPFv3 1081
Configurer les minuteries mOSPFv3 1081
Définir les voisins OSPFv3 statiques 1083
Réinitialiser les paramètres par défaut OSPFv3 1084
Envoyer les messages du journal système 1085
Supprimer les messages du journal système 1086
Calculer les coûts récapitulatifs de la route 1086
Générer une route externe par défaut dans un domaine de routage OSPFv3 1087
Configurer un préfixe de résumé IPv6 1088
Redistribuer les routes IPv6 1088
Configurer le redémarrage progressif 1090
Configurer les capacités 1091
Configuration du redémarrage progressif pour OSPFv2 1091
Configurer le redémarrage progressif de Cisco NSF pour OSPFv2 1091
Configuration de la minuterie d'attente de redémarrage progressif pour le OSPF 1092
Configuration du redémarrage progressif pour OSPFv3 1093
Configuration de la minuterie d'attente de redémarrage progressif pour OSPF 1094
Supprimer la configuration OSPFv2 1095
Supprimer la configuration OSPFv3 1095
Exemple de protocole OSPFv2 1095
Exemples de protocole OSPFv3 1097
Supervision OSPF 1098
Historique OSPF 1102

CHAPITRE 34 IS-IS 1105
À propos d'IS-IS 1105
À propos de NET 1105
Nom de domaine dynamique IS-IS 1106
Types de PDU IS-IS 1106
Fonctionnement d'IS-IS sur les circuits multiaccès 1108
Choix de l'IS désigné IS-IS 1108

Synchronisation LSPDB IS-IS 1109
Calcul du chemin le plus court IS-IS 1110
Protocole d'arrêt IS-IS 1111
Conditions préalables d'IS-IS 1111
Lignes directrices relatives à IS-IS 1112
Configurer IS-IS 1112
Activer le routage IS-IS globalement 1112
Activer l'authentification IS-IS 1116
Configurer LSP IS-IS 1120
Configurer les adresses de résumé IS-IS 1124
Configurer les interfaces passives IS-IS 1125
Configurer les interfaces IS-IS 1126
Configurer le remplissage d'interfaces Hello IS-IS 1131
Configurer la famille d'adresses IPv4 IS-IS 1133
Configurer la famille d'adresses IPv6 IS-IS 1138
Supervision IS-IS 1143
Historique d'IS-IS 1146
Exemples d'IS-IS 1146

CHAPITRE 35 EIGRP 1157
À propos d'EIGRP 1157
Lignes directrices relatives à l'EIGRP 1159
Configurer le protocole EIGRP 1160
Activer EIGRP 1160
Activer le routage Stub EIGRP 1160
Personnaliser l'EIGRP 1162
Définir un réseau pour un processus de routage EIGRP 1162
Configurer les interfaces pour l'EIGRP 1163
Configurer des interfaces passives 1165
Configurer les adresses d'agrégation du résumé sur les interfaces 1166
Modifier la valeur du délai d'interface 1166
Activer l'authentification EIGRP sur une interface 1167
Définir un voisin EIGRP 1169
Redistribuer les routes dans l'EIGRP 1170

Filtrer les réseaux dans l'EIGRP 1172
Personnaliser l'intervalle Hello et le délai de rétention dans l'EIGRP 1173
Désactiver la synthèse automatique des routes 1174
Configurer les informations par défaut dans l'EIGRP 1174
Désactiver l'horizon divisé de l'EIGRP 1175
Redémarrer le processus EIGRP 1176
Supervision de l'EIGRP 1177
Exemple pour l'EIGRP 1178
Historique d'EIGRP 1179

CHAPITRE 36 **Routage multidiffusion** 1181
À propos du routage de multidiffusion 1181
Routage de multidiffusion Stub 1181
Routage de multidiffusion PIM 1182
Prise en charge de la multidiffusion PIM propre à la source 1182
Routeur de démarrage PIM (BSR) 1182
Terminologie du routeur de démarrage PIM (BSR) 1183
Concept de groupe de multidiffusion 1184
Adresses de multidiffusion 1184
Mise en grappe 1184
Lignes directrices pour le routage de multidiffusion 1184
Routage multidiffusion activé 1185
Personnaliser le routage multidiffusion 1186
Configurer le routage de multidiffusion Stub et transférer les messages IGMP 1186
Configurer une route de multidiffusion statique 1186
Configurer des fonctionnalités IGMP 1187
Désactiver IGMP sur une interface 1187
Configurer l'appartenance au groupe IGMP 1188
Configurer un groupe IGMP joint statiquement 1188
Contrôler l'accès aux groupes de multidiffusion 1189
Limiter le nombre d'états IGMP sur une interface 1190
Modifier les messages de requête destinés aux groupes de multidiffusion 1190
Modifier la version IGMP 1192
Configurer des fonctionnalités PIM 1192

Activer et désactiver la PIM sur une interface 1192
Configurer une adresse de point de rendez-vous statique 1193
Configurer la priorité des routeurs désignés 1194
Configurer et filtrer les messages de registre PIM 1194
Configurer les intervalles des messages PIM 1195
Filtrer les voisins PIM 1195
Configurer un filtre de voisin bidirectionnel PIM 1196
Configurer l'ASA comme candidat BSR 1197
Configurer une limite de multidiffusion 1198
Supervision de PIM 1198
Exemple de routage de multidiffusion 1199
Historique du routage de multidiffusion 1200

PARTIE VI **Serveurs AAA et base de données locale** 1201

CHAPITRE 37 **AAA et base de données locale** 1203
À propos d'AAA et de la base de données locale 1203
Authentification 1203
Autorisation 1204
Comptabilité 1204
Interaction entre authentification, autorisation et traçabilité 1204
Serveurs et groupes de serveurs AAA 1204
À propos de la base de données locale 1206
Prise en charge du basculement 1207
Fonctionnement du basculement avec plusieurs serveurs dans un groupe 1208
Lignes directrices relatives à la base de données locale 1208
Ajouter un compte d'utilisateur à la base de données locale 1208
Supervision de la base de données locale 1210
Historique de la base de données locale 1211

CHAPITRE 38 **Serveurs RADIUS pour AAA** 1215
À propos des serveurs RADIUS pour AAA 1215
Méthodes d'authentification prises en charge 1215
Autorisation des utilisateurs pour les connexions VPN 1216

Ensembles d'attributs RADIUS pris en charge 1216
Attributs d'autorisation RADIUS pris en charge 1216
Attributs d'autorisation RADIUS IETF pris en charge 1226
Codes de motif de déconnexion comptable RADIUS 1227
Lignes directrices relatives aux serveurs RADIUS pour AAA 1228
Configurer les serveurs RADIUS pour AAA 1228
Configurer les groupes de serveurs RADIUS 1229
Ajouter un serveur RADIUS à un groupe 1232
Supervision des serveurs RADIUS pour AAA 1235
Historique des serveurs RADIUS pour AAA 1236

CHAPITRE 39 **Serveurs TACACS+ pour AAA** 1237
À propos des serveurs TACACS+ pour AAA 1237
Attributs TACACS+ 1237
Lignes directrices relatives aux serveurs TACACS+ pour AAA 1239
Configurer les serveurs TACACS+ 1239
Configurer les groupes de serveurs TACACS+ 1239
Ajouter un serveur TACACS+ à un groupe 1241
Supervision des serveurs TACACS+ pour AAA 1242
Historique des serveurs TACACS+ pour AAA 1243

CHAPITRE 40 **Serveurs LDAP pour AAA** 1245
À propos de LDAP et de l'ASA 1245
Fonctionnement de l'authentification avec LDAP 1245
Hiérarchie LDAP 1246
Rechercher dans la hiérarchie LDAP 1246
Lier à un serveur LDAP 1247
Cartes d'attribut LDAP 1248
Lignes directrices relatives aux serveurs LDAP pour AAA 1249
Configurer les serveurs LDAP pour AAA 1249
Configurer les cartes d'attribut LDAP 1250
Configurer les groupes de serveurs LDAP 1252
Configurer l'autorisation avec LDAP pour le VPN 1254
Supervision des serveurs LDAP pour AAA 1256

Historique des serveurs LDAP pour AAA 1256

CHAPITRE 41 **Serveurs Kerberos pour AAA** 1259

Lignes directrices relatives aux serveurs Kerberos pour AAA 1259

Configurer les serveurs Kerberos pour AAA 1259

Configurer les groupes de serveurs AAA Kerberos 1259

Ajouter des serveurs Kerberos à un groupe de serveurs Kerberos 1261

Configurer la validation du centre de distribution des clés Kerberos 1263

Superviser les serveurs Kerberos pour AAA 1264

Historique des serveurs Kerberos pour AAA 1264

CHAPITRE 42 **Configurer les serveurs RSA SecurID pour AAA** 1267

À propos des serveurs RSA SecurID 1267

Lignes directrices relatives aux serveurs RSA SecurID pour AAA 1267

Configurer les serveurs RSA SecurID pour AAA 1268

Configurer les groupes de serveurs RSA SecurID pour AAA 1268

Ajouter des serveurs RSA SecurID à un groupe de serveurs SDI 1269

Importer le fichier secret de nœud SDI 1270

Superviser les serveurs RSA SecurID pour AAA 1271

Historique des serveurs RSA SecurID pour AAA 1271

PARTIE VII **Administration système** 1273

CHAPITRE 43 **Accès de gestion** 1275

Configurer l'accès de gestion à distance 1275

Configurer l'accès SSH 1275

Activer le serveur SSH 1276

Configurer SSH pour l'accès par mot de passe 1279

Configurer SSH pour l'accès par clé publique 1280

Configurer l'accès Telnet 1285

Configurer l'accès HTTPS pour ASDM, autres clients 1286

Configurer la redirection HTTP pour l'accès ASDM ou le SSL VPN sans client 1289

Configurer l'accès de gestion sur un tunnel VPN 1289

Configurer l'accès de gestion pour FXOS sur les interfaces de données en mode plateforme Firepower 2100 1290
Modifier le délai d'expiration de la console 1292
Personnaliser une invite de l'interface de ligne de commande 1293
Configurer une bannière de connexion 1294
Définir un quota de sessions de gestion 1295
Configurer AAA pour les administrateurs système 1296
Configurer l'authentification de gestion 1296
À propos de l'authentification de gestion 1296
Configurer l'authentification pour l'interface de ligne de commandeet ASDM Access 1299
Configurer l'activation de l'authentification (mode d'exécution privilégié) 1299
Configurer l'authentification par certificat ASDM 1300
Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion 1302
Configurer l'autorisation de commande 1304
À propos de l'autorisation de commande 1305
Configurer l'autorisation de commande locale 1306
Configurer les commandes sur le serveur TACACS+ 1308
Configurer l'autorisation de commande TACACS+ 1311
Configurer une politique de mot de passe pour les utilisateurs de base de données locale 1312
Changer votre mot de passe 1315
Activer et afficher l'historique de connexion 1315
Configurer la traçabilité de l'accès de gestion 1316
Récupérer d'un verrouillage 1317
Accès au moniteur 1318
Historique de l'accès de gestion 1321

CHAPITRE 44 **Logiciels et configurations** 1331
Mettre à niveau le logiciel 1331
Charger une image à l'aide de ROMMON (ISA 3000) 1331
Mettre à niveau l'image ROMMON : ISA 3000 1333
Rétrograder votre logiciel 1334
Directives et limites en matière de rétrogradation 1334
Configuration incompatible supprimée après la rétrogradation 1336
Rétrograder l'appareil ASA 1337

Rétrograder le Firepower 2100 en mode plateforme 1338
Rétrograder le Firepower 4100/9300 1339
Rétrograder l'ISA 3000 1340
Gérer les fichiers 1340
Afficher les fichiers dans la mémoire flash 1340
Supprimer des fichiers de la mémoire flash 1341
Effacer le système de fichiers flash 1342
Configurer l'accès au fichier 1342
Configurer le mode client FTP 1342
Configurer l'ASA Secure Copy Client 1343
Configurer le chemin du client TFTP pour l'ASA 1345
Copier un fichier sur l'ASA 1345
Copier un fichier dans la configuration de démarrage ou d'exécution 1348
Définir l'image ASA, ASDM et la configuration de démarrage 1350
Sauvegarde et restauration de configurations ou d'autres fichiers 1353
Effectuer une sauvegarde ou une restauration complète du système 1353
Avant d'entreprendre la sauvegarde ou la restauration 1354
Sauvegarder le système 1355
Restaurer la sauvegarde 1356
Configurer la sauvegarde et la restauration automatiques (ISA 3000) 1358
Configurer la sauvegarde automatique (ISA 3000) 1358
Configurer la restauration automatique (ISA 3000) 1359
Sauvegarder la configuration en mode unique ou la configuration système en mode multiple 1361
Sauvegarder une configuration de contexte ou un autre fichier dans la mémoire flash 1362
Sauvegarder une configuration de contexte dans un contexte 1363
Copier la configuration à partir de l'affichage du terminal 1364
Sauvegarder les fichiers supplémentaires à l'aide des commandes d'exportation et d'importation 1364
Utiliser un script pour sauvegarder et restaurer des fichiers 1365
Avant d'utiliser des scripts de sauvegarde et de restauration 1365
Exécuter le script 1366
Exemple de script 1366
Échange à chaud d'un SSD sur Cisco Secure Firewall 1371
Historique des logiciels et des configurations 1373

CHAPITRE 45 **Automatisation de la réponse pour les événements système** 1377

À propos de l'EEG 1377

Événements pris en charge 1377

Actions sur les applets de gestionnaire d'événements 1378

Destinations de sortie 1378

Lignes directrices pour l'EEG 1379

Configurer l'EEG 1379

Créer un applet de gestionnaire d'événements et configurer les événements 1380

Configurer une action et des destinations pour la sortie d'une action 1381

Exécuter un applet de gestionnaire d'événements 1383

Suivre l'allocation de mémoire et l'utilisation de la mémoire 1384

Exemples d'EEG 1387

Supervision de l'EEG 1388

Historique de l'EEG 1388

CHAPITRE 46 **Tests et dépannage** 1391

Récupérer les mots de passe d'activation et Telnet 1391

Récupérer les mots de passe sur l'ISA 3000 1391

Récupérer les mots de passe ou les images sur l'ASA virtuel 1393

Désactiver la récupération du mot de passe pour le matériel ISA 3000 1394

Afficher les messages de débogage 1395

Capture de paquets 1395

Lignes directrices pour la capture des paquets 1395

Capturer les paquets 1396

Afficher une capture de paquets 1399

Afficher le vidage en cas de panne 1402

Afficher le vidage de la mémoire 1402

Utilisation et rapport d'utilisation du processeur (CPU) 1402

Utilisation de vCPU dans l'ASA virtuel 1402

Exemple d'utilisation du processeur 1402

Rapport d'utilisation du CPU VMware 1403

ASA virtuel et graphiques vCenter 1403

Rapports d'utilisation du CPU Amazon CloudWatch 1404

ASA virtuel et graphiques Amazon CloudWatch 1404
Rapport d'utilisation du CPU Azure 1404
Graphiques ASA virtuel et Azure 1405
Rapport d'utilisation du CPU Hyper-V 1405
Graphiques ASA virtuel et Hyper-V 1406
Rapport d'utilisation du CPU OCI 1407
ASA virtuel et graphiques OCI 1407
Tester votre configuration 1407
Tester la connectivité de base : envoi d'un ping à des adresses 1407
Ce que vous pouvez tester en utilisant le ping 1407
Choisir entre le ping ICMP et TCP 1408
Activer le protocole ICMP 1408
Envoyer un message ping à des hôtes 1410
Tester la connectivité ASA de manière systématique 1411
Tracer les routes vers les hôtes 1414
Rendre l'ASA visible sur les routes de trace 1414
Déterminer les routes de paquets 1416
Utiliser l'outil Packet Tracer pour tester la configuration de la politique 1417
Supervision des connexions 1420
Historique des tests et du dépannage 1420

PARTIE VIII **Surveillance** 1423

CHAPITRE 47 **Journalisation** 1425
À propos de la journalisation 1425
Journalisation dans le mode de contexte multiple 1426
Analyse des messages du journal système 1426
Format des messages du journal système 1427
Niveaux de gravité 1428
Filtrage des messages Syslog 1428
Classe de messages Syslog 1429
Listes de messages personnalisés 1432
Mise en grappe 1432
Lignes directrices relatives à la journalisation 1433

Configurer la journalisation 1435
Activer la journalisation 1435
Configurer une destination de sortie 1435
Envoyer des messages du journal système à un serveur externe de journal système 1435
Envoyer les messages du journal système au tampon du journal interne 1439
Envoyer des messages Syslog à une adresse courriel 1441
Envoyer les messages du journal système au gestionnaire ASDM 1442
Envoyer les messages du journal système au port de console 1444
Envoyer les messages du journal système au serveur SNMP 1444
Envoyer les messages du journal système à une session Telnet ou SSH 1444
Configurer les messages du journal système 1445
Afficher ou masquer les noms d'utilisateur non valides dans les journaux système 1445
Inclure la date et l'heure dans les messages du journal système 1445
Désactiver un message du journal système 1446
Modifier le niveau de gravité d'un message du journal système 1446
Bloquer les messages du journal système sur une unité de secours 1447
Inclure l'ID de périphérique dans les messages du journal système au format non EMBLEM 1447
Créer une liste d'événements personnalisée 1448
Configurer les filtres de journalisation 1449
Envoyer tous les messages du journal système d'une classe vers une destination de sortie spécifiée 1449
Limiter le débit de génération des messages Syslog 1450
Supervision des journaux 1450
Exemples de journalisation 1451
Historique de journalisation 1452

CHAPITRE 48 **MIB SNMP 1455**
À propos de SNMP 1455
Terminologie SNMP 1456
MIB et déroutements 1456
Identifiants d'objet SNMP 1458
Valeurs de type de prestataire physique 1460
Tableaux et objets pris en charge dans les MIB 1461
Interruptions prises en charge (notifications) 1463

Types d'interface et exemples 1468
Présentation du SNMP version 3 1469
Modèles de sécurité 1470
SNMP Groups (groupes SNMP) 1470
Utilisateurs SNMP 1470
Hôtes SNMP 1470
Différences d'implémentation entre les logiciels ASA et Cisco IOS 1471
Messagerie du journal système SNMP 1471
Services d'application et outils tiers 1471
Lignes directrices pour SNMP 1471
Configurer SNMP 1476
Activer l'agent SNMP et le serveur SNMP 1476
Configurer les déroutements SNMP 1477
Configurer un seuil d'utilisation du CPU 1478
Configurer un seuil d'interface physique 1479
Configurer les paramètres pour la version 1 ou 2c du SNMP 1479
Configurer les paramètres pour la version 3 du SNMP 1481
Configurer un groupe d'utilisateurs 1484
Associer les utilisateurs à un objet réseau 1485
Supervision SNMP 1486
Exemples de SNMP 1487
Historique de SNMP 1488

CHAPITRE 49 **Données de télémétrie et du Cisco Success Network** 1495
À propos de Cisco Success Network 1495
Plateformes prises en charge et configurations requises 1496
Comment les données de télémétrie ASA atteignent le nuage SSE 1496
Activer ou désactiver Cisco Success Network 1496
Afficher les données de télémétrie d'ASA 1497
Cisco Success Network – Données de télémétrie 1498
Déboguer les données de télémétrie 1504

CHAPITRE 50 **Alarmes pour Cisco ISA 3000** 1507
À propos des alarmes 1507

Interfaces d’entrée d’alarme 1508
Interface de sortie d'alarme 1508
Valeurs par défaut pour les alarmes 1509
Configurer les alarmes 1509
Surveillance des alarmes 1512
Historique des alarmes 1515

CHAPITRE 51 **Rapports anonymes et Smart Call Home** 1517
À propos des rapports anonymes 1517
Exigence DNS 1518
À propos de Smart Call Home 1518
S’abonner aux groupes d’alertes 1519
Attributs des groupes d’alertes 1519
Messages envoyés à Cisco par des groupes d’alertes 1520
Seuil de gravité des messages 1522
Profils d’abonnement 1523
Lignes directrices relatives aux rapports anonymes et à Smart Call Home 1524
Configurer les rapports anonymes et Smart Call Home 1525
Configurer les rapports anonymes 1526
Configurer Smart Call Home 1527
Activer Smart Call Home 1527
Déclarer et authentifier le point de confiance d’une autorité de certification 1528
Configurer les groupes d’alertes d’environnement et d’instantané 1529
Configurer l’abonnement des groupes d’alertes 1529
Configurer les coordonnées du client 1530
Configurer le serveur de messagerie 1532
Configurer la limitation de débit du trafic 1533
Envoyer des communications à Smart Call Home 1533
Configurer un profil de destination 1534
Copier un profil de destination 1535
Renommer un profil de destination 1536
Supervision des rapports anonymes et de Smart Call Home 1537
Exemples de Smart Call Home 1538
Historique des rapports anonymes et de Smart Call Home 1539

PARTIE IX **Numéro de référence** 1541

CHAPITRE 52 **Utilisation de l'interface de commande en ligne** 1543

Mode pare-feu et mode de contexte de sécurité 1543

Modes de commande et invites 1544

Formatage de la syntaxe 1545

Commandes abrégées 1546

Modification de la ligne de commande 1546

Exécution de la commande 1546

Aide sur les commandes 1546

Afficher la configuration d'exécution 1547

Filtrer la sortie de la commande show et more 1547

Redirection et ajout de la sortie de la commande show 1548

Obtention d'un nombre de lignes pour la sortie de la commande show 1549

Pagination de la sortie de commande 1550

Ajouter des commentaires 1550

Fichiers de configuration de texte 1550

Correspondance des commandes avec les lignes dans le fichier texte 1550

Commandes de mode de configuration propres aux commandes 1551

Saisies automatiques de texte 1551

Commande de ligne 1551

Commandes non incluses dans la configuration du texte 1551

Mots de passe 1551

Plusieurs fichiers de contexte de Security 1551

Ensembles de caractères pris en charge 1552

CHAPITRE 53 **Adresses, protocoles et ports** 1553

Adresses IPv4 et filtres d'adresse locale 1553

Classes 1553

Réseaux privés 1554

Filtres d'adresse locale 1554

Déterminer le filtre d'adresse locale 1554

Déterminer l'adresse à utiliser avec le filtre d'adresse locale 1555

Adresses IPv6 1557
Format d’adresses IPv6 1557
Types d’adresses IPv6 1558
Adresses de monodiffusion 1558
Multicast Address (Adresse multidiffusion) 1560
Adresse Anycast 1561
Adresses requises 1562
Préfixes de l’adresse IPv6 1562
Protocoles et applications 1563
Ports TCP et UDP 1564
Ports et protocoles locaux 1567
Types ICMP 1569



À propos de ce guide

Les rubriques suivantes expliquent comment utiliser ce guide.

- Objectifs du document, à la page lv
- Documentation associée, à la page lv
- Conventions de document, à la page lv
- Communications, services et renseignements supplémentaires, à la page lvii

Objectifs du document

L'objectif de ce guide est de vous aider à configurer les opérations générales de la gamme Secure Firewall ASA à l'aide de l'interface de ligne de commande. Ce guide ne couvre pas toutes les fonctionnalités, mais décrit uniquement les scénarios de configuration les plus courants.

Vous pouvez également configurer et superviser l'ASA à l'aide de l'Adaptive Security Device Manager (ASDM), une application d'interface graphique utilisateur basée sur le Web. ASDM comprend des assistants de configuration pour vous guider dans certains scénarios de configuration courants et une assistance en ligne pour les scénarios moins courants.

Dans ce guide, le terme « ASA » s'applique de manière générique aux modèles pris en charge, à moins que cela ne soit spécifié autrement.

Documentation associée

Pour en savoir plus, consultez *Parcourir la documentation de la gamme Cisco ASA* à l'adresse http://www.cisco.com/go/asadocs.

Conventions de document

Le présent document respecte les conventions de texte, d'affichage et d'alerte suivantes.

Conventions de texte

Convention	Indication
boldface	Les commandes, les mots clés, les étiquettes de boutons, les noms de champ et le texte saisi par l'utilisateur s'affichent dans **boldface**. Pour les commandes basées sur des menus, le chemin complet vers la commande s'affiche.
italic	Les variables, pour lesquelles vous fournissez des valeurs, sont présentées dans une police de caractères en *italique*. Le type italique est également utilisé pour les titres de documents et pour l'usage général.
`monospace`	Les sessions de terminal et les renseignements affichés par le système apparaissent en police à `espacement fixe`.
{x | y | z}	Les options de mots clés obligatoires sont regroupées entre accolades et séparées par des barres verticales.
[ ]	Les éléments entre crochets sont facultatifs.
[x | y | z]	Les options de mots clés facultatifs sont regroupées entre crochets et séparées par des barres verticales.
[ ]	Les réponses par défaut aux invites du système sont également entre crochets.
< >	Les caractères qui ne s'impriment pas, tels que les mots de passe, sont délimités par des crochets en chevron.
!, #	Un point d'exclamation (!) ou un dièse (#) au début d'une ligne de code indique une ligne de commentaire.

Alertes adressées aux lecteurs

Ce document utilise les conventions suivantes pour les alertes adressées au lecteur :

Remarque Invite le *lecteur à consulter les remarques*. Les remarques contiennent des suggestions utiles ou des références à d'autres ressources non couvertes dans le manuel.

Astuces Signifie que *les renseignements suivants vous aideront à résoudre un problème.*

Mise en garde Invite le *lecteur à être prudent*. Dans cette situation, il est possible que vous effectuiez une opération risquant d'endommager l'équipement ou d'entraîner une perte de données.

Économiseur de temps	Indique que *l'action décrite permet de gagner du temps.* Vous pouvez gagner du temps en exécutant l'action décrite dans le paragraphe.
Avertissement	**signifie que *le lecteur doit être averti.* Dans cette situation, vous pourriez effectuer une opération risquant d'entraîner des blessures corporelles.**

Communications, services et renseignements supplémentaires

- Pour recevoir des informations pertinentes et opportunes de la part de Cisco, inscrivez-vous sur le gestionnaire de profil Cisco.
- Pour obtenir les résultats commerciaux que vous recherchez avec les technologies qui comptent, visitez les services Cisco.
- Pour soumettre une demande de service, consultez le service d'assistance de Cisco.
- Pour parcourir et découvrir des applications, des produits, des solutions et des services d'entreprise sécurisés et validés, consultez Cisco Devnet.
- Pour obtenir des documents généraux sur la réseautique, la formation et la certification, consultez Cisco Press.
- Pour trouver des informations sur la garantie d'un produit ou d'une famille de produits particuliers, accédez à Cisco Warranty Finder.

Outil de recherche de bogues

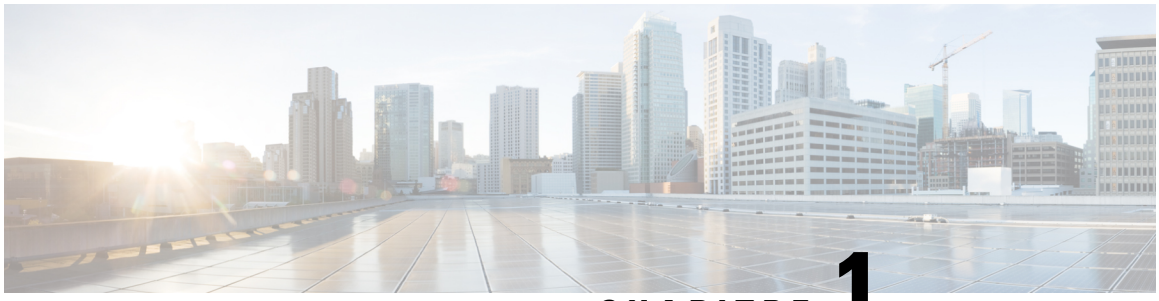
L'outil de recherche de bogues de Cisco est un outil Web qui donne accès au système de suivi des bogues de Cisco, qui conserve une liste complète des défaillances et des vulnérabilités des produits et des logiciels Cisco. Cet outil vous fournit des informations détaillées sur les défaillances de vos produits et logiciels.



PARTIE I

Mise en route de l'ASA

- Introduction à Secure Firewall ASA, à la page 1
- Pour commencer, à la page 11
- Licences : licence à clé d'autorisation de produit pour l'ISA 3000, à la page 47
- Licences : gestion des licences logicielles Smart, à la page 89
- Périphériques logiques pour le Firepower 4100/9300, à la page 175
- Mode pare-feu transparent ou routé, à la page 199



CHAPITRE 1

Introduction à Secure Firewall ASA

Le Secure Firewall ASA offre des fonctionnalités avancées de pare-feu dynamique et de concentrateur VPN dans un seul appareil. L'ASA comprend de nombreuses fonctionnalités avancées, comme des contextes de sécurité multiples (semblables aux pare-feu virtualisés), la mise en grappe (combinaison de plusieurs pare-feu en un seul pare-feu), les pare-feu transparents (couche 2) ou routés (couche 3), les moteurs d'inspection avancés, IPsec Prise en charge de VPN, de VPN SSL et de VPN SSL sans client et de nombreuses autres fonctionnalités.

- Compatibilité matérielle et logicielle, à la page 1
- Compatibilité VPN, à la page 1
- Nouvelles fonctionnalités, à la page 1
- Présentation fonctionnelle du pare-feu, à la page 4
- Présentation fonctionnelle VPN, à la page 8
- Présentation du contexte de sécurité, à la page 8
- Présentation de la mise en grappe d'ASA, à la page 9
- Services spéciaux et existants, à la page 9

Compatibilité matérielle et logicielle

Pour obtenir la liste complète du matériel et des logiciels pris en charge, consultez la section Compatibilité Cisco ASA.

Compatibilité VPN

Consultez Plateformes VPN prises en charge, série Cisco ASA.

Nouvelles fonctionnalités

Cette section énumère les nouvelles fonctionnalités de chaque version.

Remarque Les messages syslog nouveaux, modifiés et obsolètes sont répertoriés dans le guide des messages syslog.

Nouvelles fonctionnalités dans l'ASA 9.19(1)

Publication : 29 novembre 2022

Fonctionnalités	Description
Caractéristiques de la plateforme	
Secure Firewall 3105	Nous avons présenté l'ASA pour le Secure Firewall 3105.
Solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle Azure	Vous pouvez maintenant déployer la solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle sur Microsoft Azure. Consultez les fonctionnalités Interfaces pour en savoir plus.
Caractéristiques du pare-feu	
Soutien aux groupes de service du réseau	Vous pouvez désormais définir un maximum de 1 024 groupes de services réseau.
Fonctionnalités de haute disponibilité et d'évolutivité	
Suppression des propos tendancieux	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
Regroupement virtuel d'ASA sur Amazon Web Services (AWS)	L'ASA virtuel prend en charge le regroupement d'interfaces individuelles pour un maximum de 16 nœuds sur AWS. Vous pouvez utiliser la mise en grappe avec ou sans équilibreur de charge de la passerelle AWS.
Fonctionnalités de routage	
Prise en charge du redémarrage progressif de BGP pour IPv6	Nous avons ajouté la prise en charge du redémarrage progressif de BGP pour la famille d'adresses IPv6. Commandes nouvelles/modifiées : Commande existante, étendue à la prise en charge de la famille IPv6 : **ha-mode graceful-restart**
Caractéristiques de l'interface	
Prise en charge virtuelle de l'IPv6 par l'ASA	ASAv pour prendre en charge le protocole réseau IPv6 sur les plateformes du nuage privé et public. Les utilisateurs peuvent désormais : • Activer et configurer une adresse de gestion IPv6 via la configuration day0. • Attribuer des adresses IPv6 à l'aide de méthodes DHCP et statiques.

Fonctionnalités	Description
Proxy jumelé VXLAN pour l'ASA virtuel pour l'équilibreur de charges de la passerelle Azure.	Vous pouvez configurer une interface VXLAN en mode proxy apparié pour l'ASA virtuel dans Azure afin de l'utiliser avec l'équilibreur de charges de la passerelle Azure (GWLB). L'ASA virtuel définit une interface externe et une interface interne sur un seul NIC en utilisant des segments VXLAN dans un serveur mandataire jumelé. Commandes nouvelles/modifiées : **port externe, segment-id externe, port interne, segment-id interne, proxy paired**
La correction d'erreur par défaut (FEC) sur les ports fixes du Secure Firewall 3100 est passée de cl74-fc à cl108-rs pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+.	Lorsque vous définissez le FEC sur Auto sur les ports fixes du Secure Firewall 3100, le type par défaut est désormais défini sur cl108-rs au lieu de cl74-fc pour les émetteurs-récepteurs SR, CSR et LR de 25 Go. Commandes nouvelles/modifiées : **fec**
Caractéristiques de la licence	
Prise en charge de la réservation de licences virtuelles permanentes pour l'ASAv5 sur KVM et VMware	Une nouvelle commande est disponible que vous pouvez exécuter pour remplacer la licence DPP par défaut et demander à Cisco Smart Software Manager (SSM) d'envoyer une licence DPP ASAv5 lorsque vous déployez ASAv avec 2GB RAM sur KVM et VMware. Vous pouvez modifier la même commande en ajoutant la forme <*no*> pour rétablir la licence de l'ASAv5 à la licence DPP par défaut en fonction de la configuration de la mémoire vive.
Fonctions d'administration, de surveillance et de dépannage	
Pile CiscoSSH maintenant par défaut	La pile Cisco SSH est maintenant utilisée par défaut. Commandes nouvelles ou modifiées : **ssh stack ciscossh**
Fonctionnalités du VPN	
Prise en charge de l'interface de bouclage VTI	Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. La possibilité d'hériter de l'adresse IP d'une interface de bouclage au lieu d'une adresse IP configurée de manière statique a également été ajoutée. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour. Commandes nouvelles/modifiées : **tunnel source interface**, **ip unnumbered**, **ipv6 unnumbered**
Prise en charge de l'interface de tunnel virtuel dynamique (VTI dynamique)	L'ASA est améliorée grâce à l'ITV dynamique. Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. Vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur. Dynamique VTI prend en charge les rayons dynamiques (DHCP). Commandes nouvelles/modifiées : **interface virtual-Template, ip unnumbered, ipv6 unnumbered, tunnel protection ipsec policy.**
Support VTI pour EIGRP et OSPF	Le routage EIGRP et OSPFv2/v3 est désormais pris en charge sur l'interface du tunnel virtuel. Vous pouvez maintenant utiliser ces protocoles de routage pour partager les informations de routage et pour acheminer le flux de trafic à travers le tunnel VPN basé sur VTI entre les pairs.

Fonctionnalités	Description
TLS 1.3 dans le VPN d'accès à distance	Vous pouvez désormais utiliser TLS 1.3 pour chiffrer les connexions VPN d'accès à distance. TLS 1.3 ajoute la prise en charge des chiffrements suivants : • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 Cette fonctionnalité nécessite Cisco Secure Client, version 5.0.01242 ou ultérieure. Commandes nouvelles/modifiées : **sslserver-version, sslclient-version**.
Prise en charge de la double pile pour les clients tiers IKEv2	Secure Firewall ASA prend désormais en charge les demandes d'IP à double pile provenant de clients VPN d'accès à distance tiers IKEv2. Si le client VPN d'accès à distance tiers demande des adresses IPv4 et IPv6, l'ASA peut désormais attribuer les deux versions d'adresses IP à l'aide de plusieurs sélecteurs de trafic. Cette fonction permet aux clients VPN d'accès à distance tiers d'envoyer des données IPv4 et IPv6 par le biais d'un seul tunnel IPsec. Commandes nouvelles/modifiées : **show crypto ikev2 sa, show crypto ipsec sa, show vpn-sessiondb ra-ikev2-ipsec**.
Sélecteur de trafic pour l'interface VTI statique	Vous pouvez maintenant attribuer un sélecteur de trafic à une interface VTI statique. Commandes nouvelles/modifiées : **tunnel protection ipsec policy**.
Spécifier la version maximum du protocole SSL/TLS	Vous pouvez désormais spécifier la version maximum du protocole SSL/TLS que l'ASA peut utiliser en tant que client ou serveur. Commandes nouvelles ou modifiées : **ssl client-max-version, ssl client-max-version**.

Présentation fonctionnelle du pare-feu

Les pare-feu protègent les réseaux internes contre les accès non autorisés par des utilisateurs d'un réseau externe. Un pare-feu peut également protéger les réseaux internes les uns des autres, par exemple en séparant le réseau des ressources humaines du réseau des utilisateurs. Si vous avez des ressources réseau qui doivent être disponibles pour un utilisateur externe, comme un serveur Web ou FTP, vous pouvez placer ces ressources sur un réseau distinct derrière le pare-feu, appelé *zone démilitarisée* (DMZ). Le pare-feu permet un accès limité à la DMZ, mais comme celle-ci ne comprend que les serveurs publics, une attaque à cet endroit n'affecte que les serveurs et n'affecte pas les autres réseaux internes. Vous pouvez également contrôler quand les utilisateurs internes accèdent aux réseaux externes (par exemple, l'accès à Internet), en n'autorisant que certaines adresses, en exigeant une authentification ou une autorisation, ou en effectuant une coordination avec un serveur de filtrage d'URL externe.

Lorsqu'il est question de réseaux connectés à un pare-feu, le réseau *externe* se trouve devant le pare-feu, le réseau *interne* est protégé et se trouve derrière le pare-feu, et une *DMZ*, bien que située derrière le pare-feu, permet un accès limité aux utilisateurs externes. Étant donné que l'ASA vous permet de configurer de nombreuses interfaces avec des politiques de sécurité variées, y compris de nombreuses interfaces internes, de nombreuses DMZ et même de nombreuses interfaces externes si vous le souhaitez, ces termes sont utilisés dans un sens général uniquement.

Présentation de la politique de sécurité

Une politique de sécurité détermine quel trafic est autorisé à traverser le pare-feu pour accéder à un autre réseau. Par défaut, l'ASA permet au trafic de circuler librement d'un réseau interne (niveau de sécurité supérieur) vers un réseau externe (niveau de sécurité inférieur). Vous pouvez appliquer des actions au trafic pour personnaliser la politique de sécurité.

Autorisation ou refus de trafic avec critères d'accès

Vous pouvez appliquer des critères d'accès pour limiter le trafic de l'intérieur vers l'extérieur ou autoriser le trafic de l'extérieur vers l'intérieur. Pour les interfaces de groupe de ponts, vous pouvez également appliquer un critère d'accès EtherType pour autoriser le trafic non IP.

Application de la NAT

Voici quelques avantages de la NAT :

- Vous pouvez utiliser des adresses privées sur vos réseaux internes. Les adresses privées ne sont pas routables sur Internet.
- La NAT masque les adresses locales des autres réseaux afin que les agresseurs ne puissent pas découvrir l'adresse réelle d'un hôte.
- La NAT peut résoudre les problèmes de routage IP en prenant en charge le chevauchement des adresses IP.

Protection contre les fragments IP

L'ASA fournit une protection contre les fragments d'adresse IP. Cette fonctionnalité effectue le réassemblage complet de tous les messages d'erreur ICMP et le réassemblage virtuel des fragments IP restants qui sont acheminés par l'ASA. Les fragments qui échouent à la vérification de sécurité sont abandonnés et enregistrés. Le réassemblage virtuel ne peut pas être désactivé.

Application du filtrage HTTP, HTTPS ou FTP

Bien que vous puissiez utiliser des listes d'accès pour empêcher l'accès sortant à des sites Web ou à des serveurs FTP spécifiques, la configuration et la gestion de l'utilisation du Web de cette manière ne sont pas pratiques en raison de la taille et de la nature dynamique d'Internet.

Vous pouvez configurer les fonctionnalités de sécurisation du web sur l'ASA. Vous pouvez également utiliser l'ASA en conjonction avec un produit externe tel que l'appliance Cisco pour la sécurité du web (WSA).

Application de l'inspection des applications

Des plateformes d'inspection sont nécessaires pour les services qui intègrent des renseignements d'adressage IP dans le paquet de données des utilisateurs ou qui ouvrent des canaux secondaires sur des ports attribués de manière dynamique. Ces protocoles exigent que l'ASA effectue une inspection approfondie des paquets.

Application des politiques de QoS

Certains trafics réseau, comme les messages vocaux et le streaming vidéo, ne peuvent pas tolérer de longs temps de latence. La QoS est une fonctionnalité réseau qui vous permet de donner la priorité à ces types de trafic. La QoS renvoie à la capacité d'un réseau à fournir un meilleur service au trafic réseau sélectionné.

Application des limites de connexion et de la normalisation TCP

Vous pouvez limiter les connexions TCP et UDP ainsi que les connexions amorces. La limitation du nombre de connexions et de connexions amorces vous protège contre les attaques DoS. L'ASA utilise la limite amorce pour déclencher l'interception TCP, qui protège les systèmes internes contre une attaque DoS perpétrée en inondant une interface de paquets SYN de TCP. Une connexion amorce est une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination.

La normalisation TCP est une fonctionnalité composée de paramètres de connexion TCP avancés conçus pour abandonner les paquets qui n'apparaissent pas normaux.

Activation de la détection des menaces

Vous pouvez configurer la détection des menaces par analyse et la détection des menaces de base, ainsi que l'utilisation des statistiques pour analyser les menaces.

La détection des menaces de base détecte les activités qui peuvent être liées à une attaque, comme les attaques DoS, et envoie automatiquement un message de journal système.

Une attaque par analyse typique se compose d'un hôte qui teste l'accessibilité de chaque adresse IP d'un sous-réseau (en analysant de nombreux hôtes dans le sous-réseau ou en balayage de nombreux ports dans un hôte ou un sous-réseau). La fonction de détection des menaces par analyse détermine quand un hôte effectue une analyse. Contrairement à la détection d'analyse IPS qui est basée sur les signatures de trafic, la fonction de détection des menaces par analyse ASA gère une base de données étendue qui contient des statistiques d'hôte pouvant être analysées pour l'activité d'analyse.

La base de données d'hôtes suit les activités suspectes telles que les connexions sans activité de retour, l'accès à des ports de service fermés, les comportements TCP vulnérables tels que les IPID non aléatoires, etc.

Vous pouvez configurer l'ASA pour envoyer des messages de journal système sur un agresseur ou vous pouvez banir automatiquement l'hôte.

Présentation du mode pare-feu

L'ASA fonctionne dans deux modes de pare-feu différents :

- Acheminé
- Transparent

En mode routage, l'ASA est considéré comme un saut de routeur dans le réseau.

En mode transparent, l'ASA agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et n'est pas considéré comme un saut de routeur. L'ASA se connecte au même réseau sur ses interfaces interne et externe dans un « groupe de ponts ».

Vous pouvez utiliser un pare-feu transparent pour simplifier la configuration de votre réseau. Le mode transparent est également utile si vous souhaitez que le pare-feu soit visible par les agresseurs. Vous pouvez également utiliser un pare-feu transparent pour le trafic qui serait autrement bloqué en mode routé. Par exemple, un pare-feu transparent peut autoriser les flux de multidiffusion à l'aide d'une liste d'accès EtherType.

Le mode routé prend en charge le routage et le ponts intégrés. Vous pouvez donc également configurer des groupes de ponts en mode routé et acheminer le routage entre les groupes de ponts et les interfaces normales. En mode routé, vous pouvez répliquer la fonctionnalité en mode transparent; si vous n'avez pas besoin du mode de contexte multiple ou de la mise en grappe, vous pouvez envisager d'utiliser le mode routé.

Présentation de l'inspection dynamique

Tout le trafic qui passe par l'ASA est inspecté à l'aide de l'algorithme de sécurité adaptatif et est autorisé ou abandonné. Un filtre de paquet simple peut vérifier l'adresse source, l'adresse de destination et les ports appropriés, mais il ne vérifie pas si la séquence ou les indicateurs des paquets sont corrects. Un filtre vérifie également *chaque* paquet par rapport au filtre, ce qui peut être un processus lent.



Remarque La fonction de contournement d'état TCP vous permet de personnaliser le flux de paquet.

Cependant, un pare-feu dynamique comme l'ASA prend en compte l'état d'un paquet :

- S'agit-il d'une nouvelle connexion?

  S'il s'agit d'une nouvelle connexion, l'ASA doit vérifier le paquet par rapport aux listes d'accès et effectuer d'autres tâches pour déterminer si le paquet est autorisé ou refusé. Pour effectuer cette vérification, le premier paquet de la session passe par le « chemin de gestion de session » et, selon le type de trafic, il peut également passer par le « chemin de plan de commande ».

  Le chemin de gestion de session est responsable des tâches suivantes :

  - Effectuer les vérifications de la liste d'accès
  - Effectuer des recherches de route
  - Attribuer des traductions NAT (xlates)
  - Établir des sessions dans le « chemin rapide »

  L'ASA crée des flux de transfert et d'inversion dans le chemin rapide pour le trafic TCP; l'ASA crée également des renseignements sur l'état de connexion pour les protocoles sans connexion comme UDP et ICMP (lorsque vous activez l'inspection ICMP), afin qu'ils puissent également utiliser le chemin rapide.



Remarque Pour les autres protocoles IP, comme SCTP, l'ASA ne crée pas de flux de chemin inverse. Par conséquent, les paquets d'erreur ICMP qui font référence à ces connexions sont abandonnés.

  Certains paquets nécessitant une inspection de couche 7 (la charge utile des paquets doit être inspectée ou modifiée) sont transmis au chemin du plan de commande. Des moteurs d'inspection de couche 7 sont nécessaires pour les protocoles qui ont au moins deux canaux : un canal de données, qui utilise des numéros de port connus, et un canal de contrôle, qui utilise des numéros de port différents pour chaque session. Ces protocoles comprennent FTP, H.323 et SNMP.

- S'agit-il d'une connexion établie?

  Si la connexion est déjà établie, l'ASA n'a pas besoin de revérifier les paquets; la plupart des paquets correspondants peuvent passer par le chemin « rapide » dans les deux sens. Le chemin rapide est responsable des tâches suivantes :

  - Vérification de la somme de contrôle IP
  - Recherche de session

- Vérification du numéros de séquence TCP
- Traductions NAT en fonction des sessions existantes
- Ajustements des en-têtes de couche 3 et 4

Les paquets de données pour les protocoles qui nécessitent une inspection de couche 7 peuvent également passer par le chemin rapide.

Certains paquets de session établis doivent continuer à emprunter le chemin de gestion de session ou le chemin du plan de commande. Les paquets qui empruntent le chemin de gestion de session comprennent les paquets HTTP qui nécessitent une inspection ou un filtrage de contenu. Les paquets qui empruntent le chemin du plan de commande comprennent les paquets de contrôle pour les protocoles qui nécessitent une inspection de couche 7.

Présentation fonctionnelle VPN

Un VPN est une connexion sécurisée sur un réseau TCP/IP (tel qu'Internet) qui s'affiche comme une connexion privée. Cette connexion sécurisée s'appelle un tunnel. L'ASA utilise des protocoles de tunnellisation pour négocier les paramètres de sécurité, créer et gérer des tunnels, encapsuler des paquets, transmettre ou recevoir des paquets par le tunnel et les désencapsuler. L'ASA fonctionne comme un point terminal de tunnel bidirectionnel : il peut recevoir des paquets simples, les encapsuler et les envoyer à l'autre extrémité du tunnel où ils sont désencapsulés et envoyés à leur destination finale. Il peut également recevoir des paquets encapsulés, les désencapsuler et les envoyer à leur destination finale. L'ASA invoque divers protocoles standard pour remplir ces fonctions.

L'ASA remplit les fonctions suivantes :

- Établit des tunnels
- Négocie les paramètres du tunnel
- Authentifie les utilisateurs
- Attribue des adresses d'utilisateur
- Chiffre et déchiffre les données
- Gère les clés de sécurité
- Gère le transfert de données dans le tunnel
- Gère le transfert de données entrant et sortant en tant que point terminal de tunnel ou routeur

L'ASA invoque divers protocoles standard pour remplir ces fonctions.

Présentation du contexte de sécurité

Vous pouvez partitionner un ASA unique en plusieurs périphériques virtuels, appelés contextes de sécurité. Chaque contexte de sécurité est un périphérique indépendant, avec sa politique de sécurité, ses interfaces et ses administrateurs. Les contextes multiples sont similaires au fait d'avoir plusieurs périphériques autonomes. De nombreuses fonctionnalités sont prises en charge en mode de contexte multiple, notamment les tables de

routage, les fonctionnalités de pare-feu, IPS et la gestion; cependant, certaines fonctionnalités ne sont pas prises en charge. Consultez les chapitres consacrés aux fonctionnalités pour en savoir plus.

En mode de contexte multiple, l'ASA comprend une configuration pour chaque contexte qui identifie la politique de sécurité, les interfaces et presque toutes les options que vous pouvez configurer sur un périphérique autonome. L'administrateur système ajoute et gère les contextes en les configurant dans la configuration système, qui, à l'instar d'une configuration monomode, est la configuration de démarrage. La configuration système identifie les paramètres de base de l'ASA. La configuration système n'inclut aucune interface réseau ni aucun paramètre réseau pour elle-même; au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise l'un des contextes désigné comme contexte d'administration.

Le contexte d'administration est comme un contexte de sécurité, sauf que lorsqu'un utilisateur se connecte au contexte d'administration, cet utilisateur dispose de droits d'administrateur système et peut accéder au système et à tous les autres contextes.

Présentation de la mise en grappe d'ASA

La mise en grappe d'ASA vous permet de regrouper plusieurs ASA en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques.

Vous effectuez toute la configuration (à l'exception de la configuration de démarrage) sur l'unité de contrôle uniquement; la configuration est ensuite répliquée sur les unités membres.

Services spéciaux et existants

Pour certains services, la documentation se trouve en dehors des guides de configuration principaux et de l'aide en ligne.

Guides de services spéciaux

Des services spéciaux permettent à l'ASA d'interagir avec d'autres produits Cisco; par exemple, en fournissant un mandataire de sécurité pour les services téléphoniques (Unified Communications), en fournissant le filtrage du trafic réseau de zombies en conjonction avec la base de données dynamique du serveur de mise à jour de Cisco, ou en fournissant des services WCCP pour l'appliance Cisco pour la sécurité du web. Certains de ces services spéciaux sont couverts par des guides distincts :

- Guide de filtrage du trafic du réseau de zombies Cisco ASA
- Guide de mise en œuvre de Cisco ASA NetFlow
- Guide de Cisco ASA Unified Communications
- Guide de redirection du trafic WCCP Cisco ASA
- Guide de mise en œuvre des outils SNMP version 3

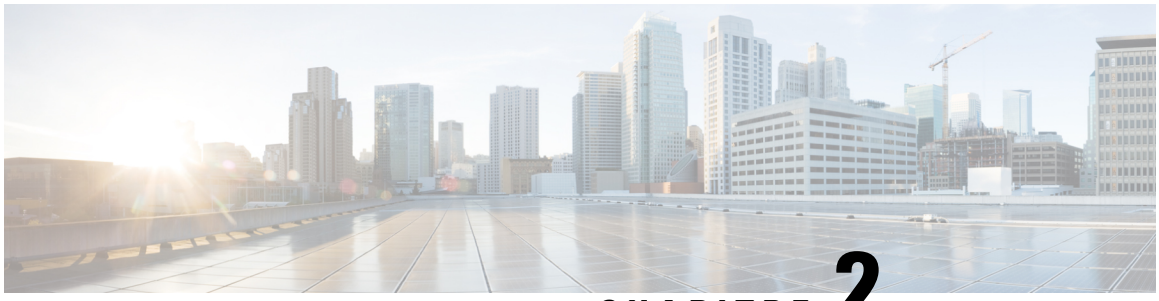
Guide des services existants

Les services existants sont toujours pris en charge sur l'ASA, mais il peut y avoir de meilleurs services de remplacement que vous pouvez utiliser à la place. Les services existants sont couverts dans un guide distinct :

Guide des fonctionnalités existantes de Cisco ASA

Ce guide comprend les chapitres suivants :

- Configuration de RIP
- Règles AAA pour l'accès au réseau
- À l'aide des outils de protection, qui comprennent la prévention de l'usurpation d'adresse IP (**ip verify reverse-path**), la configuration de la taille des fragments (**fragment**), le blocage des connexions indésirables (**shun**), la configuration des options TCP (pour ASDM) et la configuration de l'audit IP pour la prise en charge IPS de base (**ip audit**).
- Configuration des services de filtrage



CHAPITRE 2

Pour commencer

Ce chapitre décrit comment démarrer l'utilisation de votre ASA.

- Accéder à la console de l'interface de commande en ligne, à la page 11
- Configurer l'accès ASDM, à la page 18
- Démarrer ASDM, à la page 21
- Configurations d'usine par défaut, à la page 22
- Régler le Firepower 2100 en mode appareil ou plateforme, à la page 37
- Travailler avec la configuration, à la page 39
- Appliquer les modifications de configuration aux connexions, à la page 45
- Recharger l'ASA, à la page 45

Accéder à la console de l'interface de commande en ligne

Pour la configuration initiale, accédez à l'interface de ligne de commande directement à partir du port de console. Plus tard, vous pourrez configurer l'accès à distance à l'aide de Telnet ou SSH conformément à Accès de gestion, à la page 1275. Si votre système est déjà en mode de contexte multiple, l'accès au port de console vous place dans l'espace d'exécution du système.

Si vous obtenez des caractères non lisibles lors de la connexion au port de console, vérifiez les paramètres du port. S'ils sont corrects, essayez le câble avec un autre appareil en utilisant les mêmes paramètres. Si le câble est en bon état, vous devrez peut-être remplacer le matériel du port de console. Envisagez également d'essayer un autre ordinateur de travail pour établir la connexion.

Remarque Pour l'accès à la console ASA virtuel, consultez le guide de démarrage rapide ASA virtuel.

Accéder à la console de l'ISA 3000

Procédez comme suit pour accéder à la console de l'appareil.

Procédure

Étape 1 Connectez un ordinateur au port de la console à l'aide du câble de console fourni, puis connectez-vous à la console à l'aide d'un émulateur de terminal pour 9600 bauds, 8 bits de données, aucune parité, 1 bit d'arrêt, aucun contrôle de flux.

Pour plus de renseignements sur le câble de console, consultez le guide sur le matériel pour votre ASA.

Étape 2 Appuyez sur la touche **Entrée** pour afficher l'invite suivante :

```
ciscoasa>
```

Cette invite indique que vous êtes en mode EXEC utilisateur. Le mode EXEC utilisateur donne uniquement accès aux commandes de base.

Étape 3 Accédez au mode d'exécution privilégié.

enable

Vous êtes invité à en changer le mot de passe la première fois que vous entrez la commande **enable**.

Exemple :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode privilégié, entrez la commande **disable**, **exit** ou **quit** .

Étape 4 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Vous pouvez commencer à configurer l'ASA à partir du mode de configuration globale. Pour quitter le mode de configuration globale, entrez la commande **exit**, **quit** ou **end**.

Accéder à la console du mode plateforme de Firepower 2100

Le port de console Firepower 2100 se connecte à l'interface de ligne de commande de Cisco Secure Firewall eXtensible Operating System (interface de ligne de commande de FXOS). À partir de l'interface de ligne de

commande de FXOS, vous pouvez ensuite vous connecter à la console ASA, puis revenir en arrière. Si vous établissez un lien entre SSH et FXOS, vous pouvez également vous connecter à l'interface de ligne de commande d'ASA; une connexion SSH n'est pas une connexion de console, vous pouvez donc avoir plusieurs connexions ASA à partir d'une connexion SSH FXOS. De même, si vous vous connectez à l'ASA, vous pouvez vous connecter à l'interface de ligne de commande de FXOS.

Avant de commencer

Vous ne pouvez avoir qu'une seule connexion de console à la fois. Lorsque vous vous connectez à la console ASA à partir de la console FXOS, cette connexion est une connexion de console persistante, différente d'une connexion Telnet ou SSH.

Procédure

Étape 1 Connectez votre ordinateur de gestion au port de console. Firepower 2100 est livrée avec un câble série DB-9 à RJ-45, vous aurez donc besoin d'un câble série USB tiers pour établir la connexion. Assurez-vous d'installer les pilotes série USB nécessaires à votre système d'exploitation. Utilisez les paramètres de série suivants :

- 9 600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

Vous vous connectez à l'interface de ligne de commande FXOS. Entrez les informations d'identification de l'utilisateur; par défaut, vous pouvez vous connecter avec l'utilisateur **admin** et le mot de passe par défaut, **Admin123**.

Étape 2 Connectez-vous à l'ASA :

connect asa

Exemple :

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

Étape 3 Accédez au mode d'exécution privilégié.

enable

Lors de votre première saisie de la commande **enable**, vous devrez modifier le mot de passe.

Exemple :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode privilégié, entrez la commande **disable**, **exit** ou **quit** .

Étape 4 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Vous pouvez commencer à configurer l'ASA à partir du mode de configuration globale. Pour quitter le mode de configuration globale, entrez la commande **exit**, **quit** ou **end**.

Étape 5 Pour revenir à la console FXOS, entrez **Ctrl+a**, **d**.

Étape 6 Si vous vous connectez à l'aide du protocole SSH à l'ASA (après avoir configuré l'accès SSH sur l'ASA), connectez-vous à l'interface de ligne de commande de FXOS.

connect fxos

Vous serez invité à vous authentifier pour accéder à FXOS. Utilisez le nom d'utilisateur : **admin** et le mot de passe : **Admin123** par défaut. Pour revenir à l'interface de ligne de commande de l'ASA, entrez **exit** ou tapez **Ctrl-Shift-6**, **x**.

Exemple :

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Accéder à la console Firepower 1000, 2100 en mode appareil et Secure Firewall 3100

Les ports de console Firepower 1000, 2100 en mode appareil et Secure Firewall 3100 vous relient à l'interface de ligne de commande de l'ASA (contrairement à la console Firepower 2100 en mode plateforme, qui vous relie à l'interface de ligne de commande FXOS). À partir de l'interface de ligne de commande d'ASA, vous pouvez ensuite vous connecter à l'interface de ligne de commande FXOS à l'aide de Telnet à des fins de dépannage.

Procédure

Étape 1 Connectez votre ordinateur de gestion au port de console. Assurez-vous d'installer les pilotes série nécessaires à votre système d'exploitation. Utilisez les paramètres de série suivants :

- 9 600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

Vous vous connectez à l'interface de ligne de commande d'ASA. Aucun identifiant d'utilisateur n'est requis pour l'accès à la console par défaut.

Étape 2 Accédez au mode d'exécution privilégié.

enable

Lors de votre première saisie de la commande **enable**, vous devrez modifier le mot de passe.

Exemple :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Le mot de passe d'activation que vous définissez sur l'ASA est également le mot de passe de l'utilisateur **administrateur** FXOS si l'ASA ne parvient pas à démarrer et que vous passez en mode Failsafe (sécurité intégrée) dans FXOS.

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode d'exécution privilégié, entrez la commande **disable**, **exit** ou **quit**.

Étape 3 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Vous pouvez commencer à configurer l'ASA à partir du mode de configuration globale. Pour quitter le mode de configuration globale, entrez la commande **exit**, **quit** ou **end**.

Étape 4 (Facultatif) Connectez-vous au Interface de ligne de commande FXOS.

connect fxos [**admin**]

- **admin** : fournit un accès au niveau administrateur. Sans cette option, les utilisateurs ont un accès en lecture seule. Notez qu'aucune commande de configuration n'est disponible même en mode admin.

Vous n'êtes pas invité à saisir les informations d'authentification de l'utilisateur. Le nom d'utilisateur actuel de l'ASA est transmis au moyen de FXOS, et aucune connexion supplémentaire n'est requise. Pour revenir à l'interface de ligne de commande de l'ASA, entrez **exit** ou tapez **Ctrl-Shift-6**, **x**.

À l'intérieur de FXOS, vous pouvez visualiser l'activité des utilisateurs en utilisant la commande **scope security/show audit-logs**.

Exemple :

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Accéder à la console ASA sur le Châssis Firepower 4100/9300

Pour la configuration initiale, accédez à l'interface de commande en ligne en vous connectant au superviseur Châssis Firepower 4100/9300 (au port de console ou à distance à l'aide de Telnet ou de SSH), puis en vous connectant au module de sécurité ASA.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande (console ou SSH) du superviseur Châssis Firepower 4100/9300 , puis connectez-vous à l'ASA :

connect module *slot* {**console** | **telnet**}

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

La première fois que vous accédez au module, vous accédez à l'interface de ligne de commande du module FXOS. Vous devez ensuite vous connecter à l'application ASA.

connect asa

Exemple :

```
Firepower# connect module 1 console
Firepower-module1> connect asa

asa>
```

Étape 2 Accédez au mode d'exécution privilégié, qui est le niveau de privilège le plus élevé.

enable

Lors de votre première saisie de la commande **enable**, vous devrez modifier le mot de passe.

Exemple :

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa#
```

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode privilégié, entrez la commande **disable**, **exit** ou **quit** .

Étape 3 Entrer en mode de configuration globale.

configure terminal

Exemple :

```
asa# configure terminal
asa(config)#
```

Pour quitter le mode de configuration globale, entrez la commande **disable**, **exit** ou **quit**.

Étape 4 Quittez la console d'application pour l'interface de ligne de commande du module FXOS en saisissant **Ctrl-a, d**

Vous souhaiterez peut-être utiliser l'interface de ligne de commande du module FXOS à des fins de résolution de problèmes.

Étape 5 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Configurer l'accès ASDM

Cette section décrit comment accéder à ASDM avec une configuration par défaut et comment configurer l'accès si vous n'avez pas de configuration par défaut.

Utiliser la configuration d'usine par défaut pour l'accès ASDM

Avec une configuration d'usine par défaut, la connectivité ASDM est préconfigurée avec les paramètres réseau par défaut.

Procédure

Connectez-vous à ASDM en utilisant les paramètres d'interface et de réseau suivants :

- L'interface de gestion dépend de votre modèle :
  - Firepower 1010 : Management 1/1 (192.168.45.1), ou Ethernet interne 1/2 à 1/8 (192.168.1.1). Les hôtes de gestion sont limités au réseau 192.168.45.0/24 et les hôtes internes sont limités au réseau 192.168.4.0/24.
  - Firepower 1100, 2100 en mode appareil, Secure Firewall 3100 : Ethernet interne 1/2 (192.168.1.1) ou Management 1/1 (à partir de DHCP). Les hôtes internes sont limités au réseau 192.168.1.0/24. Les hôtes de gestion sont autorisés dans tous les réseaux.
  - Firepower 2100 en mode plateforme : Management 1/1 (192.168.45.1). Les hôtes de gestion sont limités au réseau 192.168.45.0/24.
  - Firepower 4100/9300 : l'interface de type de gestion et l'adresse IP de votre choix définies lors du déploiement. Les hôtes de gestion sont autorisés dans tous les réseaux.
  - ASA virtuel : Management 0/0 (défini pendant le déploiement). Les hôtes de gestion sont limités au réseau de gestion.
  - ISA 3000 : Management 1/1 (192.168.1.1). Les hôtes de gestion sont limités au réseau 192.168.1.0/24.

Remarque
Si vous passez en mode de contexte multiple, vous pouvez accéder à ASDM à partir du contexte d'administration en utilisant les paramètres réseau ci-dessus.

Sujets connexes

Configurations d'usine par défaut, à la page 22
Activer ou désactiver le mode de contexte multiple, à la page 240
Démarrer ASDM, à la page 21

Personnaliser l'accès ASDM

Utilisation cette procédure si *une ou plusieurs* des conditions suivantes s'appliquent :

- Vous n'avez pas de configuration d'usine par défaut
- Vous souhaitez modifier l'adresse IP de gestion
- Vous souhaitez passer en mode de pare-feu transparent
- Vous souhaitez passer en mode de contexte multiple

Pour le mode routé et unique, pour un accès ASDM rapide et facile, nous vous conseillons d'appliquer la configuration d'usine par défaut avec la possibilité de définir votre propre adresse IP de gestion. Utilisez la procédure de cette section uniquement si vous avez des besoins particuliers, tels que la configuration du mode transparent ou de contexte multiple, ou si vous avez une autre configuration que vous devez conserver.



Remarque Pour l'ASAv, vous pouvez configurer le mode transparent lorsque vous le déployez; cette procédure est donc principalement utile après le déploiement si vous devez effacer votre configuration, par exemple.

Procédure

Étape 1 Accédez à l'interface de ligne de commande au niveau du port de console.

Étape 2 (Facultatif) Activez le mode de pare-feu transparent :

Cette commande efface votre configuration.

firewall transparent

Étape 3 Configurez l'interface de gestion :

```
interface interface_id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

Exemple :

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

Le **niveau de sécurité** est un nombre compris entre 1 et 100, où 100 désigne le niveau le plus sécurisé.

Étape 4 (Pour les hôtes de gestion directement connectés) Définissez le pool DHCP pour le réseau de gestion :

```
dhcpd address ip_address-ip_address interface_name
```

dhcpd enable *interface_name*

Exemple :

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

Assurez-vous de ne pas inclure l'adresse de l'interface dans la plage.

Étape 5 (Pour les hôtes de gestion à distance) Configurez une route vers les hôtes de gestion :

route *management_ifc management_host_ip mask gateway_ip* **1**

Exemple :

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

Étape 6 Activez le serveur HTTP pour ASDM :

http server enable

Étape 7 Autoriser le ou les hôte(s) de gestion à accéder à ASDM :

http *ip_address mask interface_name*

Exemple :

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

Étape 8 Enregistrez la configuration :

write memory

Étape 9 (Facultatif) Définissez le mode sur plusieurs modes :

mode multiple

Lorsque vous y êtes invité, confirmez que vous souhaitez convertir la configuration existante pour en faire le contexte d'administration. Vous êtes alors invité à recharger l'ASA.

Exemples

La configuration suivante convertit le mode de pare-feu en mode transparent, configure l'interface de gestion Management 0/0 et active ASDM pour un hôte de gestion :

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
```

```
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

Sujets connexes

Rétablir les valeurs par défaut de la configuration, à la page 23
Définir le mode du pare-feu, à la page 210
Accéder à la console de l'ISA 3000, à la page 11
Démarrer ASDM, à la page 21

Démarrer ASDM

Lancez ASDM à l'aide du lancement ASDM-IDM. Le lanceur est une application téléchargée à partir de l'ASA à l'aide d'un navigateur que vous pouvez utiliser pour vous connecter à n'importe quelle adresse IP ASA. Vous n'avez pas besoin de télécharger à nouveau le lanceur si vous souhaitez vous connecter à d'autres ASA.

Dans ASDM, vous pouvez choisir une autre adresse IP ASA à gérer.

Cette section décrit comment se connecter à ASDM pour la première fois, puis lancer ASDM à l'aide du lanceur.

ASDM stocke les fichiers dans le répertoire \Users\<user_id>\.asdm, y compris le cache, le journal et les préférences, ainsi que dans le répertoire Temp, y compris les profils Secure Client (services client sécurisés).

Procédure

Étape 1 Sur le PC que vous avez spécifié comme client ASDM, saisissez l'URL suivante :

https://*asa_ip_address***/admin**

Remarque
Assurez-vous de préciser **https://** et **http://** ou simplement l'adresse IP (par défaut HTTP); l'ASA ne transfère pas automatiquement une requête HTTP vers HTTPS.

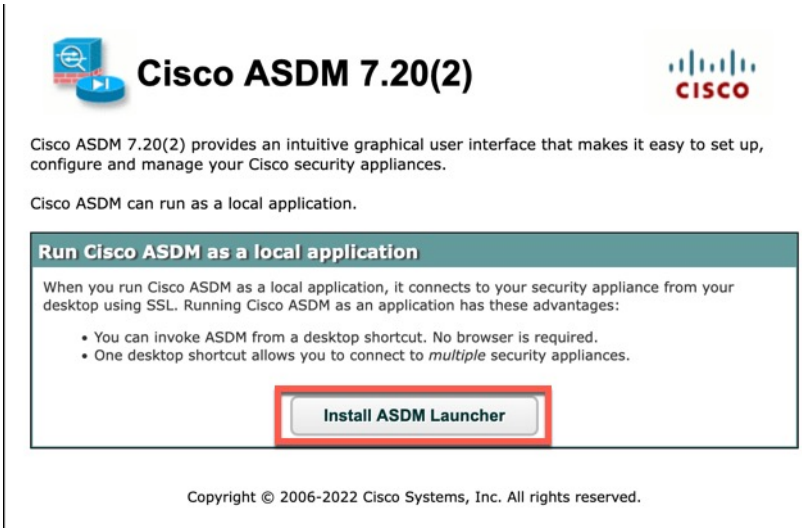
La page de lancement ASDM apparaît avec les boutons suivants :

Installer le lanceur ASDM

Étape 2 Pour télécharger le lanceur et démarrer ASDM :

a) Cliquez sur **Install ASDM Launcher**.

Illustration 1 : Installer le lanceur ASDM



b) Laissez les champs du nom d'utilisateur et du mot de passe vides (pour une nouvelle installation), puis cliquez sur **OK**.

   En l'absence d'authentification HTTPS, vous pouvez accéder à ASDM sans nom d'utilisateur et mot de passe **d'activation**, qui est vide par défaut. Lorsque vous saisissez la commande **enable** au niveau de l'interface de ligne de commande pour la première fois, vous êtes invité à modifier le mot de passe; ce comportement n'est pas appliqué lorsque vous vous connectez à ASDM. Nous vous suggérons de modifier le mot de passe d'activation dès que possible afin qu'il ne reste pas vide; voir Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet, à la page 831. **Remarque** : Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé. Même sans authentification, si vous saisissez un nom d'utilisateur et un mot de passe à l'écran de connexion (au lieu de laisser le nom d'utilisateur vide), ASDM vérifie la base de données locale à la recherche d'une correspondance.

c) Enregistrez le programme d'installation sur votre ordinateur, puis démarrez le programme d'installation. Le lanceur ASDM-IDM s'ouvre automatiquement une fois l'installation terminée.

d) Saisissez la gestion des adresses IP, le même nom d'utilisateur et mot de passe (vide pour une nouvelle installation), puis cliquez sur **OK**.

Configurations d'usine par défaut

La configuration d'usine par défaut est la configuration appliquée par Cisco aux nouveaux ASA.

- Firepower 1010 : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion ou des ports de commutation internes.
- Firepower 1100 : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion ou de l'interface interne.

- Firepower 2100 —Mode plateforme (par défaut) : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide de Cisco Secure Firewall chassis manager (anciennement Firepower Chassis Manager) et d'ASDM à partir de l'interface de gestion.

  Mode appareil : si vous passez en mode appareil, la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion ou de l'interface interne.

- Secure Firewall 3100 : la configuration d'usine par défaut permet une configuration intérieure/extérieure fonctionnelle. Vous pouvez gérer l'ASA à l'aide d'ASDM à partir de l'interface de gestion Management 1/1 ou de l'interface interne.

- Châssis Firepower 4100/9300 : lorsque vous déployez l'unité autonome ou une grappe d'ASA, la configuration d'usine par défaut configure une interface pour la gestion afin que vous puissiez vous y connecter à l'aide d'ASDM, avec lequel vous pouvez ensuite terminer votre configuration.

- ASA virtuel : en fonction de votre hyperviseur, dans le cadre du déploiement, la configuration de déploiement (les paramètres de déploiement virtuel initiaux) configure une interface pour la gestion afin que vous puissiez vous y connecter à l'aide d'ASDM, avec lequel vous pouvez ensuite terminer votre configuration. Vous pouvez également configurer des adresses IP de basculement. Vous pouvez également appliquer une configuration « d'usine par défaut » si vous le souhaitez.

- ISA 3000 : la configuration par défaut est une configuration en mode de pare-feu transparent presque complète avec toutes les interfaces internes et externes sur le même réseau; vous pouvez vous connecter à l'interface de gestion avec ASDM pour définir l'adresse IP de votre réseau. Le contournement matériel est activé pour deux paires d'interfaces .

Pour les appareils, la configuration d'usine par défaut est disponible uniquement pour le mode de pare-feu routé et le mode de contexte unique, sauf pour l'ISA 3000, où la configuration d'usine par défaut n'est disponible qu'en mode transparent. Pour l'ASA virtuel et l'Châssis Firepower 4100/9300 , vous pouvez choisir le mode transparent ou routé lors du déploiement.



Remarque En plus des fichiers image et de la configuration (masquée) par défaut, les dossiers et fichiers suivants sont standard dans la mémoire flash : log/, crypto_archive/ et coredumpinfo/coredump.cfg. La date de ces fichiers peut ne pas correspondre à celle des fichiers image dans la mémoire flash. Ces fichiers facilitent le dépannage potentiel; ils n'indiquent pas qu'une défaillance s'est produite.

Rétablir les valeurs par défaut de la configuration

Cette section décrit comment restaurer les valeurs par défaut de la configuration. Pour l'ASA virtuel, cette procédure efface la configuration de déploiement et applique la configuration suivante :

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
```

```
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

Remarque Sur le Firepower 4100/9300, la restauration de la configuration d'usine par défaut efface simplement la configuration; pour restaurer la configuration par défaut, vous devez redéployer l'ASA à partir du superviseur.

Avant de commencer

Cette fonctionnalité est disponible uniquement en mode de pare-feu routé, sauf pour l'ISA 3000, où cette commande est prise en charge uniquement en mode transparent. En outre, cette fonctionnalité est disponible uniquement en mode de contexte unique; un ASA avec une configuration effacée n'a pas de contextes définis à configurer automatiquement à l'aide de cette fonctionnalité.

Procédure

Étape 1 Restaurez les valeurs par défaut de la configuration :

configure factory-default [*ip_address* [*mask*]]

Exemple :

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

Remarque
Cette commande ne supprime pas le mode (appareil ou plateforme) actuellement défini pour Firepower 2100.

Si vous spécifiez l'*ip_address*, vous définissez l'adresse IP interne ou de l'interface de gestion, selon votre modèle, au lieu d'utiliser l'adresse IP par défaut. Consultez les directives de modèle suivantes pour savoir quelle interface est définie par l'option *ip_address* :

- Firepower 1010 : définit l'adresse IP de l'interface de **gestion**.
- Firepower 1100 : définit l'adresse IP de l'interface **interne**.
- Firepower 2100 en mode appareil : définit l'adresse IP de l'interface **interne**.
- Firepower 2100 en mode plateforme : définit l'adresse IP de l'interface de **gestion**.
- Secure Firewall 3100 : définit l'adresse IP de l'interface **interne**.
- Firepower 4100/9300 : aucun effet.
- ASA virtuel : définit l'adresse IP de l'interface de **gestion**.
- ISA 3000 : définit l'adresse IP de l'interface de **gestion**.

La commande **http** utilise le sous-réseau que vous spécifiez. De même, la plage de commandes **dhcpd address** se compose de toutes les adresses disponibles supérieures à l'adresse IP que vous spécifiez. Par exemple, si

vous spécifiez 10.5.6.78 avec un filtre d'adresse locale 255.255.255.0, la plage d'adresses DHCP sera 10.5.6.79-10.5.6.254.

Pour Firepower 1000 et Firepower 2100 en mode appareil, et Secure Firewall 3100 : cette commande efface la commande **boot system**, si elle est présente, ainsi que le reste de la configuration. Cette modification de configuration n'affecte pas l'image au démarrage : l'image actuellement chargée continue d'être utilisée.

Pour Firepower 2100 en mode plateforme : ce modèle n'utilise pas la commande **boot system**; les paquets sont gérés par FXOS.

Pour tous les autres modèles : cette commande efface la commande **boot system**, si elle est présente, ainsi que le reste de la configuration. La commande **boot system** vous permet de démarrer à partir d'une image en particulier. La prochaine fois que vous rechargez l'ASA après avoir restauré la configuration d'usine, il démarre à partir de la première image de la mémoire flash interne; si vous n'avez pas d'image dans la mémoire flash interne, l'ASA ne démarre pas.

Exemple :

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
WARNING: The new maximum-session limit will take effect after the running-config is saved
and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Étape 2 Enregistrez la configuration par défaut dans la mémoire flash :

write memory

Cette commande enregistre la configuration d'exécution à l'emplacement par défaut pour la configuration de démarrage, même si vous avez précédemment configuré la commande **boot** pour définir un emplacement différent; lorsque la configuration a été effacée, ce chemin a également été effacé.

Restaurer la configuration du déploiement de l'ASA virtuel

Cette section décrit comment restaurer la configuration du déploiement de l'ASA virtuel (Day0).

Procédure

Étape 1 Pour le basculement, mettez hors tension l'unité en veille.

Pour empêcher l'unité en veille de devenir active, vous devez l'éteindre. Si vous la laissez activée, lorsque vous effacez la configuration de l'unité active, l'unité en veille devient active. Lorsque l'ancienne unité active se recharge et se reconnecte via la liaison de basculement, l'ancienne configuration sera synchronisée à partir de la nouvelle unité active, effaçant ainsi la configuration de déploiement souhaitée.

Étape 2 Restaurez la configuration de déploiement après le rechargement. Pour le basculement, saisissez cette commande sur l'unité active :

write erase

Remarque
L'ASA virtuel démarre l'image en cours d'exécution, de sorte que vous n'êtes pas revenu à l'image de démarrage d'origine. Pour utiliser l'image de démarrage d'origine, consultez la commande **boot image**.

N'enregistrez pas la configuration.

Étape 3 Rechargez l'ASA virtuel et chargez la configuration de déploiement :

reload

Étape 4 Pour le basculement, mettez sous tension l'unité en veille.

Après le rechargement de l'unité active, mettez sous tension l'unité en veille. La configuration de déploiement se synchronisera avec l'unité en veille.

Configuration par défaut de Firepower 1010

La configuration d'usine par défaut du Firepower 1010 concerne les éléments suivants :

- **Commutateur matériel** : Ethernet 1/2 à 1/8 appartient à VLAN 1
- **inside→outside (flux de trafic)** : Ethernet 1/1 (externe), VLAN1 (interne)
- **management** (gestion) : Management 1/1 (gestion), adresse IP 192.168.45.1
- **adresse IP externe** de DHCP, **adresse IP interne** — 192.168.1.1
- **serveur DHCP** sur interface interne, interface de gestion
- **Voie de routage par défaut** depuis l'extérieur de DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes de gestion sont limités au réseau 192.168.45.0/24 et les hôtes internes sont limités au réseau 192.168.4.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur

- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
```

```
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Configuration par défaut de Firepower 1100

La configuration d'usine par défaut du Firepower 1100 concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, **adresse IP interne**—192.168.1.1
- **gestion**—Management 1/1 (gestion), adresse IP de DHCP
- **serveur DHCP** sur interface interne
- **Routes par défaut** depuis l'extérieur de DHCP, gestion DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes internes sont limités au réseau 192.168.1.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
```

```
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Configuration par défaut du mode plateforme de Firepower 2100

Vous pouvez configurer Firepower 2100 pour un fonctionnement en mode plateforme; le mode appareil est le mode par défaut.

Remarque Pour les versions antérieures à la version 9.13 (1), le mode plateforme était la seule option par défaut. Si vous effectuez une mise à niveau à partir du mode plateforme, ce mode est maintenu.

Configuration ASA

La configuration d'usine par défaut d'ASA sur Firepower 2100 concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, adresse IP interne — 192.168.1.1
- **serveur DHCP** sur interface interne
- **Voie de routage par défaut** depuis l'extérieur de DHCP
- **management** (gestion) : Management 1/1 (gestion), adresse IP 192.168.45.1
- Accès **ASDM** : hôtes de gestion.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Initialisation du trafic de **gestion FXOS** : le châssis FXOS peut initier le trafic de gestion sur l'interface externe ASA.
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Management1/1
  management-only
```

```
  nameif management
  security-level 100
  ip address 192.168.45.1 255.255.255.0
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
ip-client outside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

Configuration FXOS

La configuration d'usine par défaut de FXOS sur Firepower 2100 concerne les éléments suivants :

- **Interface Management 1/1** : adresse IP 192.168.45.45
- **Passerelle par défaut** : interfaces de données ASA
- **Firewall Chassis Manager et l'accès SSH** : depuis le réseau du gestionnaire uniquement.
- **Nom d'utilisateur par défaut** : le nom d'utilisateur **admin** et le mot de passe par défaut **Admin123**.
- **Serveur DHCP** : plage d'adresses IP de clients 192.168.45.10-192.168.45.12
- **NTP** : Serveurs NTP de Cisco : 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
- Serveurs **DNS** , OpenDNS : 208.67.222.222, 208.67.220.220
- **Ethernet 1/1 et Ethernet 1/2** : activés

Configuration par défaut du mode appareil de Firepower 2100

Le Firepower 2100 fonctionne en mode Appliance (appareil) par défaut.

Remarque Pour les versions antérieures à la version 9.13 (1), le mode plateforme était la seule option par défaut. Si vous effectuez une mise à niveau à partir du mode plateforme, le mode plateforme est maintenu.

La configuration d'usine par défaut pour le Firepower 2100 en mode appareil concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, **adresse IP interne**—192.168.1.1
- **adresse IP de gestion** : depuis DHCP—Management 1/1 (gestion)
- **serveur DHCP** sur interface interne
- **Routes par défaut** depuis l'extérieur de DHCP, gestion DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes internes sont limités au réseau 192.168.1.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

```
!
```

Configuration par défaut de Secure Firewall 3100

La configuration d'usine par défaut pour Secure Firewall 3100 concerne les éléments suivants :

- **flux de trafic interne→externe** : Ethernet 1/1 (externe), VLAN1 (interne)
- **adresse IP externe** de DHCP, **adresse IP interne**—192.168.1.1
- **gestion**—Management 1/1 (gestion), adresse IP de DHCP
- **serveur DHCP** sur interface interne
- **Routes par défaut** depuis l'extérieur de DHCP, gestion DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes internes sont limités au réseau 192.168.1.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Serveurs **DNS** : les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

```
!
```

Configuration par défaut de Châssis Firepower 4100/9300

Lorsque vous déployez l'ASA sur le Châssis Firepower 4100/9300 , vous pouvez prédéfinir de nombreux paramètres qui vous permettent de vous connecter à l'interface de gestion à l'aide d'ASDM. Une configuration typique comprend les paramètres suivants :

- Interface de gestion :
  - Interface de type de gestion de votre choix définie sur le superviseur Châssis Firepower 4100/9300
  - Nommée « gestion »
  - Adresse IP de votre choix
  - Niveau de sécurité 0
  - Gestion uniquement
- Route par défaut via l'interface de gestion
- Accès ASDM : tous les hôtes autorisés.

La configuration d'une unité autonome comprend les commandes suivantes. Pour une configuration supplémentaire des unités en grappe, consultez Créer une grappe ASA, à la page 461.

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

Configuration par défaut d'ISA 3000

La configuration d'usine par défaut pour ISA 3000 concerne les éléments suivants :

- **Transparent firewall mode** (Mode de pare-feu transparent) : un pare-feu transparent est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.
- **1 Bridge Virtual Interface** (1 interface virtuelle de pont) : toutes les interfaces membres se trouvent dans le même réseau (**adresse IP *non* préconfigurée; vous devez le définir pour qu'il corresponde à votre réseau**) : GigabitEthernet 1/1 (outside1), GigabitEthernet 1/2 (inside1), GigabitEthernet 1/3 (inside2), GigabitEthernet 1/4 (inside2)

- Toutes les interfaces **internes et externes** peuvent communiquer entre elles.
- Interface **Management 1/1** : 192.168.1.1/24 pour l'accès à ASDM.
- **DHCP** pour les clients sur la gestion.
- Accès **ASDM** : hôtes de gestion.
- L'option **Hardware bypass** (Contournement matériel) est activée pour les paires d'interfaces suivantes : GigabitEthernet 1/1 et 1/2; GigabitEthernet 1/3 et 1/4



Remarque Lorsque l'ISA 3000 perd de l'alimentation et passe en mode de contournement matériel, seules les paires d'interfaces ci-dessus peuvent communiquer; inside1 et inside2, et outside1 et outside2 ne peuvent plus communiquer. Toutes les connexions existantes entre ces interfaces seront perdues. Lorsque l'alimentation revient, il y a une brève interruption de la connexion lorsque l'ASA prend en charge les flux.

La configuration comprend les commandes suivantes :

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
```

```
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management
```

Configuration du déploiement ASA virtuel

Lorsque vous déployez l'ASA virtuel, vous pouvez prédéfinir de nombreux paramètres qui vous permettent de vous connecter à l'interface de gestion Management 0/0 à l'aide d'ASDM. Une configuration typique comprend les paramètres suivants :

- Mode de pare-feu routé ou transparent
- Interface de gestion Management 0/0 :
  - Nommée « gestion »
  - Adresse IP ou DHCP
  - Niveau de sécurité 0
- Route statique pour l'adresse IP de l'hôte de gestion (s'il ne se trouve pas sur le sous-réseau de gestion)
- Serveur HTTP activé ou désactivé
- Accès HTTP pour l'adresse IP de l'hôte de gestion
- (Facultatif) Adresses IP de liaison de basculement pour GigabitEthernet 0/8 et adresse IP de secours Management 0/0
- Serveur DNS
- Jeton d'ID de licence Smart
- Niveau de débit de la licence Smart et niveau de fonctionnalité Essentials
- (Facultatif) URL et port du mandataire HTTP Smart Call Home
- (Facultatif) Paramètres de gestion SSH :
  - Adresses IP du client
  - Nom d'utilisateur et mot de passe locaux
  - Authentification requise pour SSH à l'aide de la base de données LOCALE
- (Facultatif) API REST activée ou désactivée

Remarque Pour enregistrer avec succès l'ASA virtuel auprès de l'autorité de licence de Cisco, l'ASA virtuel nécessite un accès Internet. Vous devrez peut-être effectuer une configuration supplémentaire après le déploiement pour obtenir un accès Internet et un enregistrement de licence réussi.

Consultez l'exemple de configuration suivant pour une unité autonome :

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

Remarque La licence Essentials était appelée licence « Standard ».

Consultez l'exemple de configuration suivant pour une unité principale dans une paire de basculement :

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
```

```
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

Régler le Firepower 2100 en mode appareil ou plateforme

Le Firepower 2100 exécute un système d'exploitation sous-jacent appelé le FXOS. Vous pouvez exécuter Firepower 2100 dans les modes suivants :

- Mode appareil (par défaut) : le mode appareil vous permet de configurer tous les paramètres de l'ASA. Seules les commandes de dépannage avancées sont disponibles à partir de l'interface de ligne de commande de FXOS.
- Mode plateforme : lorsque vous êtes en mode plateforme (Platform), vous devez configurer les paramètres de fonctionnement de base et les paramètres de l'interface matérielle dans FXOS. Ces paramètres comprennent l'activation des interfaces, l'établissement de canaux EtherChannels, du protocole NTP, de la gestion des images, etc. Vous pouvez utiliser l'interface web Firewall Chassis Manager ou l'interface de ligne de commande FXOS. Vous pouvez ensuite configurer votre politique de sécurité dans le système d'exploitation ASA en utilisant ASDM ou l'interface de ligne de commande de l'ASA.

Cette procédure vous explique comment changer de mode.

Mise en garde Lorsque vous modifiez le mode, vous devez recharger le système, et la configuration est effacée. La configuration par défaut est appliquée au rechargement. Assurez-vous de conserver une copie de la configuration d'origine pour référence.

Vous observez que les commandes **clear configure all** et **configure factory-default** ne suppriment pas le mode actuel.

Avant de commencer

Vous ne pouvez changer de mode qu'au niveau de l'interface de ligne de commande.

Procédure

Étape 1 (Facultatif) Sauvegardez votre configuration actuelle. Consultez Sauvegarde et restauration de configurations ou d'autres fichiers, à la page 1353

Bien qu'il existe de légères différences entre une configuration en mode appareil et une configuration en mode plateforme, une copie de l'ancienne configuration peut constituer un bon point de départ. Par exemple, en mode plateforme, la configuration du protocole NTP, du système DNS et du canal EtherChannel ne fait pas partie de la configuration de l'ASA; elle ne sera donc pas incluse dans votre sauvegarde, mais la plupart des autres paramètres de l'ASA sont valides pour les deux modes.

Étape 2 Affichez le mode actuel.

show fxos mode

Exemple :

```
ciscoasa(config)# show fxos mode
Mode is currently set to appliance
```

Étape 3 Définissez le mode selon le mode plateforme.

no fxos mode appliance

write memory

reload

Après avoir défini le mode, vous devez enregistrer la configuration et recharger le périphérique. Avant le rechargement, vous pouvez rétablir la valeur d'origine du mode sans interruption.

Mise en garde
Lorsque vous rechargez, la configuration est effacée. La configuration par défaut est appliquée au rechargement.

Exemple :

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Étape 4 Définissez le mode selon le mode appareil.

fxos mode appliance

write memory

reload

Après avoir défini le mode, vous devez enregistrer la configuration et recharger le périphérique. Avant le rechargement, vous pouvez rétablir la valeur d'origine du mode sans interruption.

Mise en garde
Lorsque vous rechargez, la configuration est effacée. La configuration par défaut est appliquée au rechargement.

Exemple :

```
ciscoasa(config)# fxos mode appliance
Mode set to appliance mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684
```

```
23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Travailler avec la configuration

Cette section décrit comment utiliser la configuration. Les renseignements de cette section s'appliquent aux contextes de sécurité uniques et multiples, sauf lorsque cela est indiqué.

À propos de la configuration de démarrage et de la configuration en cours d'exécution

Startup Configuration (configuration de démarrage)

Lorsque l'ASA démarre, il charge la configuration à partir d'un fichier texte appelé configuration de démarrage. Ce fichier réside par défaut en tant que fichier masqué dans la mémoire flash interne. Vous pouvez toutefois spécifier un fichier différent pour la configuration de démarrage qui réside dans le système de fichiers visible. Utilisez la commande suivante pour spécifier une nouvelle configuration de démarrage :

boot config {**disk0:/** | **disk1:/**} [*path/*]*filename*

Enregistrez le nouvel emplacement :

write memory

Par exemple :

```
ciscoasa (config)# boot config disk0:/startup.cfg
ciscoasa (config)# write memory
```

Utilisation de configurations volumineuses

L'espace disponible dans le répertoire de démarrage masqué est limité. Si votre configuration est très volumineuse (par exemple, plus de 16 Mo), vous ne pourrez pas enregistrer la configuration de démarrage. Dans ce cas, vous devez utiliser la commande **boot config** pour enregistrer la configuration de démarrage dans le système de fichiers visible. Par exemple, si vous chargez une configuration volumineuse dans la mémoire en cours d'exécution et que vous essayez de l'enregistrer, le message d'erreur suivant peut s'afficher si vous saisissez **write memory** et que la configuration est trop volumineuse :

```
%Erreur d'écriture. nvRAM:/startup-config (pas d'espace gauche sur le périphérique :)
```

Dans ce cas, assurez-vous de réenregistrer la configuration en cours d'exécution dans un nouvel emplacement de fichier avant de recharger l'ASA. Sinon, l'ASA risque de ne pas charger la configuration complète.

Running Configuration (configuration en cours d'exécution)

Lorsque vous saisissez une commande, la modification n'est appliquée qu'à la configuration en cours d'exécution dans la mémoire. Vous devez enregistrer manuellement la configuration en cours d'exécution dans la configuration de démarrage pour que vos modifications soient conservées après un rechargement.

Enregistrer les modifications de configuration

Cette section décrit comment enregistrer votre configuration.

Enregistrer les modifications de configuration en mode de contexte unique

Pour enregistrer la configuration en cours d'exécution dans la configuration de démarrage, procédez comme suit.

Procédure

Enregistrez la configuration en cours d'exécution dans la configuration de démarrage :

write memory

Remarque
La commande **copy running-config startup-config** est équivalente à la commande **write memory**.

Enregistrer les modifications de configuration en mode de contexte multiple

Vous pouvez enregistrer chaque configuration de contexte (et de système) séparément, ou vous pouvez enregistrer toutes les configurations de contexte en même temps.

Enregistrer chaque contexte et système séparément

Utilisez la procédure suivante pour enregistrer la configuration système ou du contexte.

Procédure

À partir du contexte ou du système, enregistrez la configuration en cours d'exécution dans la configuration de démarrage :

write memory

Pour le mode de contexte multiple, les configurations de démarrage de contexte peuvent résider sur des serveurs externes. Dans ce cas, l'ASA enregistre la configuration sur le serveur que vous avez identifié dans l'URL de contexte, sauf pour une URL HTTP ou HTTPS, qui ne vous permet pas d'enregistrer la configuration sur le serveur.

Remarque
La commande **copy running-config startup-config** est équivalente à la commande **write memory**.

Enregistrer toutes les configurations de contexte en même temps

Utilisez la procédure suivante pour enregistrer simultanément toutes les configurations de contexte ainsi que la configuration système.

Procédure

À partir de l'espace d'exécution du système, enregistrez la configuration en cours d'exécution dans la configuration de démarrage pour tous les contextes et la configuration système :

write memory all [**/noconfirm**]

Si vous ne saisissez pas le mot clé **/noconfirm**, l'invite suivante s'affiche :

```
Are you sure [Y/N]:
```

Après avoir saisi **Y**, l'ASA enregistre la configuration système et chaque contexte. Les configurations de démarrage de contexte peuvent résider sur des serveurs externes. Dans ce cas, l'ASA enregistre la configuration sur le serveur que vous avez identifié dans l'URL de contexte, sauf pour une URL HTTP ou HTTPS, qui ne vous permet pas d'enregistrer la configuration sur le serveur.

Après que l'ASA a enregistré chaque contexte, le message suivant s'affiche :

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Parfois, un contexte n'est pas enregistré en raison d'une erreur. Consultez les renseignements suivants pour les erreurs :

- Pour les contextes qui ne sont pas enregistrés en raison d'une mémoire faible, le message suivant s'affiche :

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- Pour les contextes qui ne sont pas enregistrés, car la destination à distance est inaccessible, le message suivant s'affiche :

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- Pour les contextes qui ne sont pas enregistrés, car le contexte est verrouillé, le message suivant s'affiche :

  ```
  Unable to save the configuration for the following contexts as these contexts are locked.
  context 'a' , context 'x' , context 'z' .
  ```

  Un contexte n'est verrouillé que si un autre utilisateur enregistre déjà la configuration ou est en train de supprimer le contexte.

- Pour les contextes qui ne sont pas enregistrés, car la configuration de démarrage est en lecture seule (par exemple, sur un serveur HTTP), le rapport de messages suivant est imprimé à la fin de tous les autres messages :

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context 'a' , context 'b' , context 'c' .
  ```

- Pour les contextes qui ne sont pas enregistrés en raison de mauvais secteurs dans la mémoire flash, le message suivant s'affiche :

```
The context 'context a' could not be saved due to Unknown errors
```

Copier la configuration de démarrage dans la configuration en cours d'exécution

Utilisez l'une des commandes suivantes pour copier une nouvelle configuration de démarrage dans la configuration en cours d'exécution :

- **copy startup-config running-config**

  Fusionne la configuration de démarrage avec la configuration en cours d'exécution. Une fusion ajoute toutes les nouvelles commandes de la nouvelle configuration à la configuration en cours d'exécution. Si les configurations sont identiques, aucune modification ne se produit. Si des commandes sont en conflit ou si des commandes influent sur le fonctionnement du contexte, l'effet de la fusion dépend de la commande. Vous pourriez obtenir des erreurs ou des résultats inattendus.

- **reload**

  Recharge l'ASA, qui charge la configuration de démarrage et supprime la configuration en cours d'exécution.

- **clear configure all** and then **copy startup-config running-config**

  Charge la configuration de démarrage et supprime la configuration en cours d'exécution sans nécessiter un rechargement.

Afficher la configuration

Les commandes suivantes vous permettent d'afficher les configurations en cours d'exécution et de démarrage :

- **show running-config**

  Affiche la configuration en cours d'exécution.

- **show running-config** *command*

  Affiche la configuration en cours d'exécution d'une commande spécifique.

- **show startup-config**

  Affiche la configuration de démarrage.

Effacer et supprimer les paramètres de configuration

Pour effacer les paramètres, entrez l'une des commandes suivantes :

- **clear configure** *configurationcommand* [*level2configurationcommand*]

Efface toute la configuration pour une commande spécifiée. Si vous ne souhaitez effacer la configuration que pour une version spécifique de la commande, vous pouvez saisir une valeur pour *level2configurationcommand*.

Par exemple, pour effacer la configuration de toutes les commandes **aaa**, saisissez la commande suivante :

```
ciscoasa(config)# clear configure aaa
```

Pour effacer la configuration uniquement des commandes **aaa authentication**, saisissez la commande suivante :

```
ciscoasa(config)# clear configure aaa authentication
```

- **no** *configurationcommand* [*level2configurationcommand*] *qualifier*

  Désactive les paramètres ou les options spécifiques d'une commande. Dans ce cas, vous utilisez la commande **no** pour supprimer la configuration spécifique identifiée par *qualifier*.

  Par exemple, pour supprimer une commande **access-list** spécifique, saisissez suffisamment de commandes pour l'identifier de façon unique; vous devrez peut-être saisir la commande complète :

```
ciscoasa(config)# no access-list abc extended permit icmp any any object-group obj_icmp_1
```

- **write erase**

  Efface la configuration de démarrage.

Remarque Pour l'ASA virtuel, cette commande restaure la configuration de déploiement après un rechargement. Pour effacer complètement la configuration, utilisez la commande **clear configure all**.

- **clear configure all**

  Efface la configuration d'exécution.

Remarque En mode de contexte multiple, si vous entrez **clear configure all**, vous supprimez également tous les contextes et empêchez leur exécution. Les fichiers de configuration de contexte ne sont pas effacés et restent dans leur emplacement d'origine.

Remarque Pour Firepower 1000 et Firepower 2100 en mode appareil, et Secure Firewall 3100 : cette commande efface la commande **boot system**, si elle est présente, ainsi que le reste de la configuration. Cette modification de configuration n'affecte pas l'image au démarrage : l'image actuellement chargée continue d'être utilisée.

Pour Firepower 2100 en mode plateforme : ce modèle n'utilise pas la commande **boot system**; les paquets sont gérés par FXOS.

Pour tous les autres modèles : cette commande efface la commande **boot system**, si elle est présente, ainsi que le reste de la configuration. La commande **boot system** vous permet de démarrer à partir d'une image spécifique, y compris une image sur la carte de mémoire flash externe. La prochaine fois que vous rechargez l'ASA, il démarre à partir de la première image de la mémoire flash interne; si vous n'avez pas d'image dans la mémoire flash interne, l'ASA ne démarre pas.

Remarque Cette commande ne supprime pas le mode (appareil ou plateforme) actuellement défini pour Firepower 2100.

Créer des fichiers de configuration texte hors ligne

Ce guide décrit comment utiliser l'interface de ligne de commande pour configurer l'ASA; lorsque vous enregistrez des commandes, les modifications sont écrites dans un fichier texte. Au lieu d'utiliser l'interface de ligne de commande, vous pouvez modifier un fichier texte directement sur votre ordinateur et coller une configuration à l'invite de ligne de commande du mode de configuration dans son intégralité ou ligne par ligne. Vous pouvez également télécharger un fichier texte dans la mémoire flash interne de l'ASA. Consultez Logiciels et configurations, à la page 1331 pour en savoir plus sur le téléchargement du fichier de configuration sur l'ASA.

Dans la plupart des cas, les commandes décrites dans ce guide sont précédées d'une invite d'interface de ligne de commande. L'invite dans l'exemple suivant est « ciscoasa(config)# » :

```
ciscoasa(config)# context a
```

Dans le fichier de configuration texte, vous n'êtes pas invité à saisir des commandes, l'invite est donc omise comme suit :

```
context a
```

Pour en savoir plus sur le formatage du fichier, consultez Utilisation de l'interface de commande en ligne, à la page 1543.

Appliquer les modifications de configuration aux connexions

Lorsque vous apportez des modifications à la configuration de la politique de sécurité, toutes les *nouvelles* connexions utilisent la nouvelle politique de sécurité. Les connexions existantes continuent d'utiliser la politique qui était configurée au moment de l'établissement de la connexion. La sortie de la commande **show** pour les anciennes connexions reflète l'ancienne configuration et, dans certains cas, n'inclura pas de données sur les anciennes connexions.

Par exemple, si vous supprimez une **politique de service** QoS d'une interface, puis ajoutez une version modifiée, la commande **show service-policy** affiche uniquement les compteurs QoS associés aux nouvelles connexions qui correspondent à la nouvelle politique de service; les connexions existantes sur l'ancienne politique ne s'affichent plus dans la sortie de la commande.

Pour vous assurer que toutes les connexions utilisent la nouvelle politique, vous devez déconnecter les connexions actuelles afin qu'elles puissent se reconnecter à l'aide de la nouvelle politique.

Pour déconnecter les connexions, saisissez la commande suivante :

- **clear conn** [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip* [*-src_ip*] [**netmask** *mask*]] [**port** *src_port* [*-src_port*]] [**address** *dest_ip* [*-dest_ip*] [**netmask** *mask*]] [**port** *dest_port* [*-dest_port*]]

  Cette commande met fin aux connexions, quel que soit leur état. Reportez-vous à la commande **show conn** pour afficher toutes les connexions actuelles.

  Sans arguments, cette commande efface toutes les connexions de transit. Pour effacer également les connexions vers la boîte (y compris votre session de gestion actuelle), utilisez le mot clé **all**. Pour effacer des connexions spécifiques en fonction de l'adresse IP source, de l'adresse IP de destination, du port et/ou du protocole, vous pouvez spécifier les options souhaitées.

Recharger l'ASA

Pour recharger l'ASA, suivez la procédure ci-dessous.

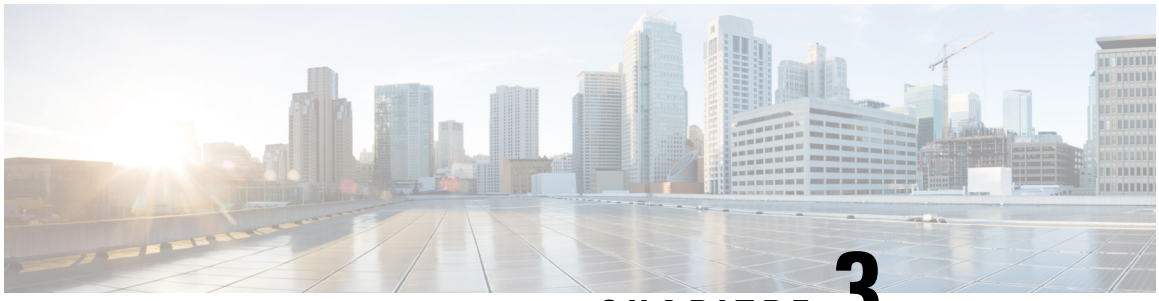
La commande **reload** n'est pas répliquée sur les nœuds de données pour la mise en grappe ou sur l'unité de secours/secondaire pour le basculement.

En mode de contexte multiple, vous pouvez seulement recharger à partir de l'espace d'exécution du système.

Procédure

Rechargez l'ASA.

reload



CHAPITRE 3

Licences : licence à clé d'autorisation de produit pour l'ISA 3000

Une licence spécifie les options qui sont activées sur un ASA donné. Ce document décrit les licences de clé d'autorisation de produit (PAK) pour l'ISA 3000. Pour d'autres modèles, consultez Licences : gestion des licences logicielles Smart, à la page 89.

- À propos des licences PAK, à la page 47
- Lignes directrices relatives aux licences PAK, à la page 56
- Configurer les licences PAK, à la page 57
- Configurer une licence partagée (Secure Client (services client sécurisés) 3 et versions antérieures), à la page 62
- Licences de fonctionnalités prises en charge par modèle, à la page 70
- Supervision des licences PAK, à la page 71
- Historique des licences PAK, à la page 81

À propos des licences PAK

Une licence spécifie les options qui sont activées sur un ASA donné. Elle est représentée par une clé d'activation qui est une valeur de 160 bits (5 mots de 32 bits ou 20 octets). Cette valeur encode le numéro de série (une chaîne de 11 caractères) et les fonctionnalités activées.

Licence préinstallée

Par défaut, votre ASA est livré avec une licence déjà installée. Cette licence peut être la licence de base, à laquelle vous souhaitez ajouter d'autres licences, ou toutes vos licences peuvent déjà être installées, selon ce que vous avez commandé et ce que votre prestataire a installé pour vous.

Sujets connexes

Supervision des licences PAK, à la page 71

Licence permanente

Vous pouvez installer une clé d'activation permanente. La clé d'activation permanente comprend toutes les fonctionnalités sous licence en une seule clé. Si vous installez également des licences à durée limitée, l'ASA combine les licences permanentes et à durée limitée en une licence en cours d'exécution.

Sujets connexes

Association des licences permanentes et à durée limitée, à la page 48

Licences à durée limitée

En plus des licences permanentes, vous pouvez acheter des licences à durée limitée ou recevoir une licence d'évaluation d'une durée limitée. Par exemple, vous pouvez acheter une licence Secure Client (services client sécurisés) Premium à durée limitée pour gérer les pics à court terme du nombre d'utilisateurs SSL VPN simultanés.

Lignes directrices relatives à l'activation de la licence à durée limitée

- Vous pouvez installer plusieurs licences à durée limitée, y compris plusieurs licences pour la même fonctionnalité. Cependant, une seule licence à durée limitée par fonctionnalité peut être *active* à la fois. La licence inactive reste installée et prête à l'emploi. Par exemple, si vous installez une licence Secure Client (services client sécurisés) Premium de 1 000 sessions et une licence Secure Client (services client sécurisés) Premium de 2 500 sessions, une seule de ces licences peut être active.
- Si vous activez une licence d'évaluation qui comporte plusieurs fonctionnalités dans la clé, vous ne pouvez pas activer une autre licence à durée limitée pour l'une des fonctionnalités incluses.

Fonctionnement de la minuterie des licences à durée limitée

- La minuterie des licences à durée limitée commence le compte à rebours lorsque vous l'activez sur l'ASA.
- Si vous cessez d'utiliser la licence à durée limitée avant son expiration, la minuterie s'arrête. La minuterie ne redémarre que lorsque vous réactivez la licence à durée limitée.
- Si la licence à durée limitée est active et que vous arrêtez l'ASA, la minuterie cesse le compte à rebours. La licence à durée limitée ne commence à compter que lorsque l'ASA est en cours d'exécution. Le paramètre de l'horloge système n'a pas d'incidence sur la licence; seul le temps de disponibilité de l'ASA est pris en compte dans la durée de la licence.

Association des licences permanentes et à durée limitée

Lorsque vous activez une licence à durée limitée, les fonctionnalités des licences permanentes et à durée limitée se combinent pour former la licence d'exécution. La façon dont les licences permanentes et à durée limitée se combinent dépend du type de licence. Le tableau suivant répertorie les règles de combinaison pour chaque licence de fonctionnalité.

Remarque Même lorsque la licence permanente est utilisée, si la licence à durée limitée est active, son compte continue.

Tableau 1 : Règles de combinaison de licences à durée limitée

Fonctionnalité à durée limitée	Règle de licence combinée
Sessions Premium Secure Client (services client sécurisés)	La valeur la plus élevée est utilisée, qu'elle soit à durée limitée ou permanente. Par exemple, si la licence permanente est de 1 000 sessions et que la licence à durée limitée est de 2 500 sessions, les 2 500 sessions sont activées. Généralement, vous n'installerez pas une licence à durée limitée ayant une capacité inférieure à la licence permanente, mais si vous le faites, la licence permanente est utilisée.
Sessions de mandataire pour les communications unifiées	Les sessions de licences à durée limitée sont ajoutées aux sessions permanentes, jusqu'à la limite de plateformes. Par exemple, si la licence permanente est de 2 500 sessions et que la licence à durée limitée est de 1 000 sessions, 3 500 sessions sont activées tant que la licence à durée limitée est active.
Tous les autres	La valeur la plus élevée est utilisée, qu'elle soit à durée limitée ou permanente. Pour les licences dont l'état est activé ou désactivé, la licence ayant l'état activé est utilisée. Pour les licences à niveaux numériques, la valeur la plus élevée est utilisée. Généralement, vous n'installerez pas une licence à durée limitée ayant une capacité inférieure à la licence permanente, mais si vous le faites, la licence permanente est utilisée.

Sujets connexes

Supervision des licences PAK, à la page 71

Empilage des licences à durée limitée

Dans de nombreux cas, vous devrez peut-être renouveler votre licence temporaire et effectuer une transition transparente de l'ancienne licence à la nouvelle. Pour les fonctionnalités qui ne sont disponibles qu'avec une licence à durée limitée, il est particulièrement important que la licence n'expire pas avant que vous puissiez appliquer la nouvelle licence. L'ASA vous permet d'*empiler* des licences à durée limitée afin que vous n'ayez pas à vous soucier de l'expiration de la licence ou de la perte de temps sur vos licences en raison de l'installation de la nouvelle licence plus tôt.

Lorsque vous installez une licence à durée limitée identique à celle déjà installée, les licences sont combinées et la durée est égale à la durée combinée.

Par exemple :

1. Vous installez une licence Secure Client (services client sécurisés) Premium de 8 semaines de 1 000 sessions et l'utilisez pendant 2 semaines (il reste 6 semaines).
2. Vous installez ensuite une autre licence de 8 semaines de 1 000 sessions, et les licences se combinent pour offrir 1 000 sessions pendant 14 semaines (8 semaines plus 6 semaines).

Si les licences ne sont pas identiques (par exemple, une licence Secure Client (services client sécurisés) Premium de 1 000 sessions et une licence de 2 500 sessions), elles ne sont *pas* combinées. Comme une seule licence à durée limitée par fonctionnalité peut être active, une seule des licences peut être active.

Bien que les licences non identiques ne se combinent pas, lorsque la licence actuelle expire, l'ASA active automatiquement une licence installée de la même fonctionnalité, si elle est disponible.

Sujets connexes

Activer ou désactiver les clés, à la page 61
Échéance de la licence à durée limitée, à la page 50

Échéance de la licence à durée limitée

Lorsque la licence actuelle d'une fonctionnalité expire, l'ASA active automatiquement une licence installée de la même fonctionnalité, si elle est disponible. Si aucune autre licence à durée limitée n'est disponible pour cette fonctionnalité, la licence permanente est utilisée.

Si vous avez plusieurs licences supplémentaires à durée limitée installées pour une fonctionnalité, l'ASA utilise la première licence qu'il trouve; la licence utilisée n'est pas configurable par l'utilisateur et dépend des opérations internes. Si vous préférez utiliser une licence autre que celle activée par l'ASA, vous devez activer manuellement la licence de votre choix.

Par exemple, vous disposez d'une licence Secure Client (services client sécurisés) Premium à durée limitée de 2 500 sessions (active), d'une licence Secure Client (services client sécurisés) Premium à durée limitée de 1 000 sessions (inactive) et d'une licence permanente Secure Client (services client sécurisés) Premium de 500 sessions. Lorsque la licence de 2 500 sessions expire, l'ASA active la licence de 1 000 sessions. Après l'expiration de la licence de 1 000 sessions, l'ASA utilise la licence permanente de 500 sessions.

Sujets connexes

Activer ou désactiver les clés, à la page 61

Remarques relatives à la licence

Les sections suivantes contiennent des renseignements supplémentaires sur les licences.

LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement

La licence Secure Client Advantage ou Premier est une licence multi-utilisation que vous pouvez appliquer à plusieurs ASA, qui partagent tous un ensemble d'utilisateurs comme spécifié par la licence. La licence VPN client sécurisé uniquement s'applique à un ASA spécifique. Consultez https://www.cisco.com/go/license et attribuez la clé PAK séparément à chaque ASA. Lorsque vous appliquez la clé d'activation résultante à un ASA, elle active les fonctionnalités VPN au maximum autorisé, mais le nombre réel d'utilisateurs uniques pour tous les ASA partageant la licence ne doit pas dépasser la limite de licence. Pour obtenir plus de renseignements, consultez la section :

- Guide de commande Cisco Secure Client (services client sécurisés)
- Foire aux questions (FAQ) Secure Client (services client sécurisés) Licensing

Remarque La licence Secure Client Premier est la seule licence Secure Client Premier prise en charge pour le mode de contexte multiple. De plus, en mode de contexte multiple, cette licence doit être appliquée à chaque unité d'une paire de basculement; la licence n'est pas agrégée.

Autre licence VPN

Les autres homologues VPN comprennent les types de VPN suivants :

- VPN d'accès à distance IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv2

Cette licence est incluse dans la licence de base.

Nombre total de sessions VPN combinées, tous types

- Le nombre total d'homologues VPN est le nombre maximum d'homologues VPN autorisés pour les homologues Secure Client (services client sécurisés) et autres homologues VPN combinés. Par exemple, si le total est de 1 000, vous pouvez autoriser 500 homologues Secure Client (services client sécurisés) et 500 autres homologues VPN simultanément; ou 700 homologues Secure Client (services client sécurisés) et 300 autres VPN; ou utiliser les 1 000 pour Secure Client (services client sécurisés). Si vous dépassez le nombre total d'homologues VPN, vous pouvez surcharger l'ASA. Assurez-vous donc de dimensionner votre réseau de manière appropriée.

Équilibrage de la charge VPN

L'équilibrage de charges VPN nécessite une licence de cryptage renforcé (3DES/AES).

Licences VPN existantes

Reportez-vous au contrat de licence de l'utilisateur final supplémentaire pour Secure Client (services client sécurisés) pour obtenir tous les renseignements pertinents sur les licences.

Remarque La licence Secure Client Premier est la seule licence Secure Client (services client sécurisés) prise en charge pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante.

Licence de chiffrement

Si le cryptage renforcé est activé, vous ne pouvez pas utiliser DES.

Nombre total de sessions de mandataire TLS

Chaque session de mandataire TLS pour l'inspection vocale chiffrée est prise en compte dans la limite de licences TLS.

D'autres applications qui utilisent des sessions de mandataire TLS ne sont pas prises en compte dans la limite du TLS, par exemple, le mandataire Mobility Advantage (qui ne nécessite pas de licence).

Certaines applications peuvent utiliser plusieurs sessions pour une connexion. Par exemple, si vous configurez un téléphone avec un Cisco Unified Communications Manager principal et de secours, il y a 2 connexions de mandataire TLS.

Vous définissez indépendamment la limite de mandataire TLS à l'aide de la commande **tls-proxy maximum-sessions** ou dans ASDM, en utilisant le volet **Configuration > Firewall (Pare-feu) > Unified Communications (Communications unifiées) > TLS Proxy (Mandataire TLS)**. Pour afficher les limites de votre modèle, saisissez la commande **tls-proxy maximum-sessions ?**. Lorsque vous appliquez une licence de mandataire TLS supérieure à la limite de mandataire TLS par défaut, l'ASA définit automatiquement la

limite de mandataire TLS pour correspondre à la licence. La limite de mandataire TLS a priorité sur la limite de la licence; si vous définissez la limite de mandataire TLS pour qu'elle soit inférieure à la licence, vous ne pouvez pas utiliser toutes les sessions de votre licence.

Remarque Pour les licences dont la référence se termine par « K8 » (par exemple, les licences de moins de 250 utilisateurs), les sessions de mandataire TLS sont limitées à 1 000. Pour les licences dont la référence se termine par « K9 » (par exemple, les licences de 250 utilisateurs ou plus), la limite de mandataire TLS dépend de la configuration, jusqu'à la limite du modèle. K8 et K9 indiquent si la licence est restreinte pour l'exportation : la licence K8 n'est pas limitée tandis que la licence K9 est restreinte.

Si vous effacez la configuration (à l'aide de la commande **clear configure all**, par exemple), la limite de mandataire TLS est définie par défaut pour votre modèle; si cette valeur par défaut est inférieure à la limite de licence, vous verrez un message d'erreur pour utiliser la commande **tls-proxy maximum-sessions** afin d'augmenter à nouveau la limite (dans ASDM, utilisez le volet **TLS Proxy** (Mandataire TLS)). Si vous utilisez le basculement et saisissez la commande **write standby** ou dans ASDM, utilisez **File (Fichier) > Save Running Configuration to Standby Unit (Enregistrer la configuration d'exécution sur l'unité en veille)** sur l'unité principale pour forcer une synchronisation de la configuration; la commande **clear configure all** est générée automatiquement sur l'unité secondaire, vous pouvez donc voir le message d'avertissement sur l'unité secondaire. Étant donné que la synchronisation de la configuration restaure la limite de mandataire TLS définie sur l'unité principale, vous pouvez ignorer l'avertissement.

Vous pouvez également utiliser des sessions de chiffrement SRTP pour vos connexions :

- Pour les licences K8, les sessions SRTP sont limitées à 250.
- Pour les licences K9, il n'y a pas de limite.

Remarque Seuls les appels qui nécessitent un chiffrement ou un déchiffrement pour un support sont pris en compte dans la limite du SRTP; si la transmission est définie pour l'appel, même si les deux segments sont des SRTP, ils ne sont pas pris en compte dans la limite.

Nombre maximum de VLAN

Pour qu'une interface soit prise en compte dans la limite de VLAN, vous devez lui attribuer un VLAN. Par exemple :

```
interface gigabitethernet 0/0.100
vlan 100
```

Licences partagées Secure Client (services client sécurisés) Premium (AnyConnect 3 et versions antérieures)

Remarque La fonctionnalité de licence partagée sur l'ASA n'est pas prise en charge avec les licences AnyConnect 4 et ultérieures. Les licences Secure Client (services client sécurisés) sont partagées et ne nécessitent plus de serveur partagé ni de licence de participant.

Une licence partagée vous permet d'acheter un grand nombre de sessions Secure Client (services client sécurisés) Premium et de partager les sessions, selon les besoins, entre un groupe d'ASA en configurant l'un des ASA en tant que serveur de licences partagées et les autres en tant que participants aux licences partagées.

Licences de basculement

À quelques exceptions près, les unités de basculement ne nécessitent pas la même licence sur chaque unité. Pour les versions antérieures, consultez le document de licence de votre version.

Exigences et exceptions en matière de licence de basculement

Modèle	Exigence de licence
ISA 3000	Licence Security Plus sur les deux unités. **Remarque** Chaque unité doit avoir la même licence de chiffrement.

Remarque Une clé permanente valide est requise; dans de rares cas sur l'ISA 3000, votre clé d'authentification PAK peut être supprimée. Si votre clé est constituée uniquement de 0, vous devez réinstaller une clé d'authentification valide avant que le basculement puisse être activé.

Association des licences de basculement

Pour les paires de basculement, les licences de chaque unité sont combinées en une seule licence de grappe en cours d'exécution. Si vous achetez des licences distinctes pour chaque unité, la licence combinée utilise les règles suivantes :

- Pour les licences qui ont des niveaux numériques, comme le nombre de sessions, les valeurs des licences de chaque unité sont combinées jusqu'à la limite de la plateforme. Si toutes les licences utilisées sont à durée limitée, les licences sont décomptées simultanément.

  Par exemple, pour le basculement :

  - Vous avez deux ASA avec 10 sessions de mandataire TLS installées sur chacun; les licences seront combinées pour un total de 20 sessions de mandataire TLS.

- Vous avez un ASA avec 1 000 sessions de mandataire TLS et un autre avec 2 000 sessions; comme la limite de plateformes est de 2 000, la licence combinée autorise 2 000 sessions de mandataire TLS.

- Pour les licences dont l'état est activé ou désactivé, la licence ayant l'état activé est utilisée.
- Pour les licences à durée limitée qui sont activées ou désactivées (et qui n'ont pas de niveaux numériques), la durée est la durée combinée de toutes les licences. L'unité principale/de contrôle compte d'abord sa licence, et à son expiration, l'unité secondaire/de données commence à décompter sa licence, et ainsi de suite.

Sujets connexes

Supervision des licences PAK, à la page 71

Perte de communication entre les unités de basculement

Si les unités perdent la communication pendant plus de 30 jours, chaque unité revient à la licence installée localement. Pendant le délai de grâce de 30 jours, la licence en cours d'exécution combinée continue d'être utilisée par toutes les unités.

Si vous rétablissez la communication pendant le délai de grâce de 30 jours, pour les licences à durée limitée, le temps écoulé est soustrait de la licence principale/de contrôle; si la licence principale/de contrôle expire, la licence secondaire/de données commence seulement à être décomptée.

Si vous ne rétablissez pas la communication pendant la période de 30 jours, pour les licences à durée limitée, le temps est soustrait de toutes les licences des unités, si elles sont installées. Elles sont traitées comme des licences distinctes et ne bénéficient pas de la licence combinée. Le délai écoulé comprend le délai de grâce de 30 jours.

Mise à niveau des paires de basculement

Étant donné que les paires de basculement ne nécessitent pas la même licence sur les deux unités, vous pouvez appliquer de nouvelles licences à chaque unité sans temps d'arrêt. Si vous appliquez une licence permanente qui nécessite un rechargement, vous pouvez basculer vers l'autre unité pendant le rechargement. Si les deux unités nécessitent un rechargement, vous pouvez les recharger séparément pour éviter les temps d'arrêt.

Sujets connexes

Activer ou désactiver les clés, à la page 61

Aucun modèle de chiffrement des données utiles

Vous pouvez acheter certains modèles sans chiffrement des données utiles. Pour l'exportation vers certains pays, le chiffrement des données utiles ne peut pas être activé sur la série ASA. Le logiciel ASA détecte un modèle sans chiffrement des données utiles et désactive les fonctionnalités suivantes :

- Communications unifiées
- VPN

Vous pouvez toujours installer la licence de cryptage renforcé (3DES/AES) pour l'utiliser avec les connexions de gestion. Par exemple, vous pouvez utiliser ASDM HTTPS/SSL, SSHv2, Telnet et SNMPv3.

Lorsque vous affichez la licence, les licences VPN et de communications unifiées ne seront pas répertoriées.

Sujets connexes

Supervision des licences PAK, à la page 71

FAQ sur les licences

Puis-je activer plusieurs licences à durée limitée?

Oui. Vous pouvez utiliser une seule licence à durée limitée par fonctionnalité à la fois.

Puis-je « cumuler » des licences à durée limitée afin que, lorsque la durée expire, la licence suivante soit automatiquement utilisée?

Oui. Pour les licences identiques, la durée est cumulée lorsque vous installez plusieurs licences à durée limitée. Pour les licences non identiques (par exemple, une licence Secure Client (services client sécurisés) Premium de 1 000 sessions et une licence de 2 500 sessions), l'ASA active automatiquement la licence à durée limitée suivante qu'il trouve pour la fonctionnalité.

Puis-je installer une nouvelle licence permanente tout en conservant une licence à durée limitée active?

Oui. L'activation d'une licence permanente n'affecte pas les licences à durée limitée.

Pour le basculement, puis-je utiliser un serveur de licences partagées comme unité principale et le serveur de sauvegarde de licences partagées comme unité secondaire?

Non. L'unité secondaire dispose de la même licence d'exécution que l'unité principale; dans le cas du serveur de licences partagées, une licence serveur est requise. Le serveur de sauvegarde nécessite une licence de participant. Le serveur de sauvegarde peut se trouver dans une paire de basculement distincte composée de deux serveurs de sauvegarde.

Dois-je acheter les mêmes licences pour l'unité secondaire d'une paire de basculement?

Non. À partir de la version 8.3(1), vous n'avez pas besoin d'avoir des licences correspondantes sur les deux unités. En règle générale, vous achetez une licence uniquement pour l'unité principale; l'unité secondaire hérite de la licence principale lorsqu'elle devient active. Dans le cas où vous avez également une licence distincte sur l'unité secondaire (par exemple, si vous avez acheté des licences correspondantes pour des logiciels antérieurs à la version 8.3), les licences sont combinées en une licence de grappe de basculement en cours d'exécution, jusqu'aux limites du modèle.

Puis-je utiliser une licence Secure Client (services client sécurisés) Premium à durée limitée ou permanente en plus d'une licence AnyConnect Premium partagée?

Oui. La licence partagée est utilisée uniquement après l'épuisement des sessions de la licence installée localement (à durée limitée ou permanente).

Remarque Sur le serveur de licences partagées, la licence Secure Client (services client sécurisés) Premium permanente n'est pas utilisée; vous pouvez toutefois utiliser une licence à durée limitée en même temps que la licence du serveur de licences partagées. Dans ce cas, les sessions de licence à durée limitée ne sont disponibles que pour les sessions Secure Client (services client sécurisés) Premium locales; elles ne peuvent pas être ajoutées au groupe de licences partagées pour être utilisées par les participants.

Lignes directrices relatives aux licences PAK

Directives relatives au mode contextuel

En mode de contexte multiple, appliquez la clé d'activation dans l'espace d'exécution du système.

Directives en matière de basculement

Consultez Licences de basculement, à la page 53.

Directives sur les modèles

- Les licences Smart sont prises en charge sur l'ASA virtuel uniquement.
- Les licences partagées ne sont pas prises en charge sur l'ASA virtuel, l'ASA 5506-X, l'ASA 5508-X et l'ASA 5516-X.
- Les ASA 5506-X et ASA 5506W-X ne prennent pas en charge les licences à durée limitée.

Lignes directrices relatives à la mise à niveau et à la rétrogradation

Votre clé d'activation reste compatible si vous effectuez une mise à niveau vers la dernière version à partir de n'importe quelle version précédente. Cependant, vous pourriez avoir des problèmes si vous souhaitez conserver la capacité de rétrogradation :

- Rétrogradation à la version 8.1 ou antérieure : après la mise à niveau, si vous activez des licences de fonctionnalités supplémentaires qui ont été introduites *avant la version 8.2*, la clé d'activation continue d'être compatible avec les versions antérieures si vous effectuez une rétrogradation. Cependant, si vous activez des licences de fonctionnalités qui ont été introduites dans la version *8.2 ou ultérieure*, la clé d'activation n'est pas rétrocompatible. Si vous avez une clé de licence incompatible, consultez les lignes directrices suivantes :
  - Si vous avez déjà saisi une clé d'activation dans une version antérieure, l'ASA utilise cette clé (sans aucune des nouvelles licences que vous avez activées dans la version 8.2 ou ultérieure).
  - Si vous avez un nouveau système et que vous n'avez pas de clé d'activation antérieure, vous devez demander une nouvelle clé d'activation compatible avec la version antérieure.
- Rétrogradation à la version 8.2 ou antérieure : la version 8.3 a introduit une utilisation plus robuste des clés temporelles ainsi que des modifications des licences de basculement :
  - Si vous avez plusieurs clés d'activation temporelles actives, lorsque vous effectuez une rétrogradation, seule la dernière clé temporelle activée peut être active. Toutes les autres clés sont désactivées. Si la dernière licence à durée limitée concerne une fonctionnalité introduite dans la version 8.3, cette licence reste toujours la licence active même si elle ne peut pas être utilisée dans les versions antérieures. Saisissez la clé permanente ou une clé temporelle valide.
  - Si vous avez des licences incompatibles avec une paire de basculement, la rétrogradation désactivera le basculement. Même si les clés correspondent, la licence utilisée ne sera plus une licence combinée.
  - Si vous avez installé une licence à durée limitée, mais qu'elle concerne une fonctionnalité introduite dans la version 8.3, cette licence à durée limitée restera active après la rétrogradation. Vous devez saisir à nouveau la clé permanente pour désactiver la licence à durée limitée.

Directives supplémentaires

- La clé d'activation n'est pas stockée dans votre fichier de configuration; elle est stockée sous forme de fichier caché dans la mémoire flash.
- La clé d'activation est liée au numéro de série de l'appareil. Les licences de fonctionnalités ne peuvent pas être transférées entre les périphériques (sauf en cas de défaillance matérielle). Si vous devez remplacer votre périphérique en raison d'une défaillance matérielle et qu'il est couvert par le TAC de Cisco, communiquez avec l'équipe chargée des licences de Cisco afin de transférer votre licence existante vers le nouveau numéro de série. L'équipe chargée des licences de Cisco vous demandera le numéro de référence de la clé d'autorisation du produit et le numéro de série existant.
- Le numéro de série utilisé pour la licence est celui indiqué dans la sortie **show version**. Ce numéro de série est différent de celui du châssis indiqué à l'extérieur du matériel. Le numéro de série du châssis est utilisé pour l'assistance technique, mais pas pour les licences.
- Une fois achetée, vous ne pouvez pas retourner une licence pour obtenir un remboursement ou une licence mise à niveau.
- Sur une seule unité, vous ne pouvez pas ajouter deux licences distinctes pour la même fonctionnalité; par exemple, si vous achetez une licence SSL VPN de 25 sessions, puis achetez ultérieurement une licence de 50 sessions, vous ne pouvez pas utiliser 75 sessions; vous pouvez utiliser un maximum de 50 sessions. (Vous pourriez acheter une licence plus importante à un prix de mise à niveau, par exemple de 25 à 75 sessions; ce type de mise à niveau doit se différencier de l'ajout de deux licences distinctes).
- Bien que vous puissiez activer tous les types de licence, certaines fonctionnalités sont incompatibles entre elles. Dans le cas de la licence AnyConnect Essentials, la licence est incompatible avec les licences suivantes : licence AnyConnect Premium, licence AnyConnect Premium partagée et licence d'évaluation de point d'accès avancée. Par défaut, si vous installez la licence AnyConnect Essentials (si elle est disponible pour votre modèle), elle est utilisée à la place des licences ci-dessus. Vous pouvez désactiver la licence AnyConnect Essentials dans la configuration pour restaurer l'utilisation des autres licences à l'aide de **webvpn**, puis avec la commande **no anyconnect-essentials** .

Configurer les licences PAK

Cette section décrit comment obtenir une clé d'activation et comment l'activer. Vous pouvez également désactiver une clé.

Commander des licences PAK et obtenir une clé d'activation

Pour installer une licence sur l'ASA, vous avez besoin de clés d'autorisation de produit, que vous pouvez ensuite enregistrer auprès de Cisco.com pour obtenir une clé d'activation. Vous pouvez ensuite saisir la clé d'activation sur l'ASA. Vous avez besoin d'une clé d'autorisation de produit distincte pour chaque licence de fonctionnalité. Les clés PAK sont combinées pour vous donner une clé d'activation unique. Vous avez peut-être reçu toutes vos clés de licence PAK dans la boîte de votre appareil. L'ASA dispose de la licence de base ou Security Plus, ainsi que de la licence de cryptage renforcé (3DES/AES), si vous remplissez les conditions requises pour son utilisation. Si vous devez demander manuellement la licence de cryptage renforcé (qui est gratuite), consultez la page http://www.cisco.com/go/license.

Avant de commencer

Lorsque vous achetez une ou plusieurs licences pour l'appareil, vous les gérez dans le Cisco Smart Software Manager :

https://software.cisco.com/#module/SmartLicensing

Si vous n'avez pas encore de compte, configurez un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.

Procédure

Étape 1 Pour acheter des licences supplémentaires, rendez-vous sur http://www.cisco.com/go/ccw. Consultez le guide de commande et la FAQ Secure Client (services client sécurisés) suivants :

- Guide de commande Cisco Secure Client (services client sécurisés)
- Foire aux questions (FAQ) Secure Client (services client sécurisés) Licensing

Après avoir commandé une licence, vous recevrez un courriel avec une clé d'autorisation de produit (PAK). Pour les licences Secure Client (services client sécurisés), vous recevez une clé PAK multiutilisation que vous pourrez appliquer à plusieurs ASA partageant le même ensemble de séances de l'utilisateur. Le courriel de la PAK peut prendre plusieurs jours dans certains cas.

Étape 2 Utilisez la commande suivante pour obtenir le numéro de série de votre ASA.

show version | grep Serial

Le numéro de série utilisé pour la licence est différent de celui du châssis indiqué à l'extérieur du matériel. Le numéro de série du châssis est utilisé pour l'assistance technique, mais pas pour les licences.

Étape 3 Pour obtenir la clé d'activation, accédez au site Web de la licence suivant :

http://www.cisco.com/go/license

Étape 4 Saisissez les renseignements suivants lorsque vous y êtes invité :

- Clé d'autorisation de produit (si vous avez plusieurs clés, saisissez d'abord l'une des clés. Vous devez saisir chaque clé en tant que processus distinct.)
- Le numéro de série de votre ASA
- Votre adresse courriel

Une clé d'activation est automatiquement générée et envoyée à l'adresse courriel que vous fournissez. Cette clé comprend toutes les fonctionnalités que vous avez enregistrées jusqu'à présent pour les licences permanentes. En ce qui concerne les licences à durée déterminée, chacune possède une clé d'activation distincte.

Étape 5 Si vous disposez de clés d'autorisation de produit supplémentaires, répétez le processus pour chaque clé d'autorisation de produit. Après avoir saisi toutes les clés d'autorisation de produit, la clé d'activation finale fournie comprend toutes les fonctionnalités permanentes que vous avez enregistrées.

Étape 6 Installez la clé d'activation conformément à Activer ou désactiver les clés, à la page 61.

Obtenir une licence de cryptage renforcé

Pour utiliser ASDM (et de nombreuses autres fonctionnalités), vous devez installer la licence de cryptage renforcé (3DES/AES). Si votre ASA n'est pas livré avec la licence de cryptage renforcé préinstallée, vous pouvez en demander une gratuitement. Vous devez bénéficier d'une licence de cryptage renforcé en fonction de votre pays.

Procédure

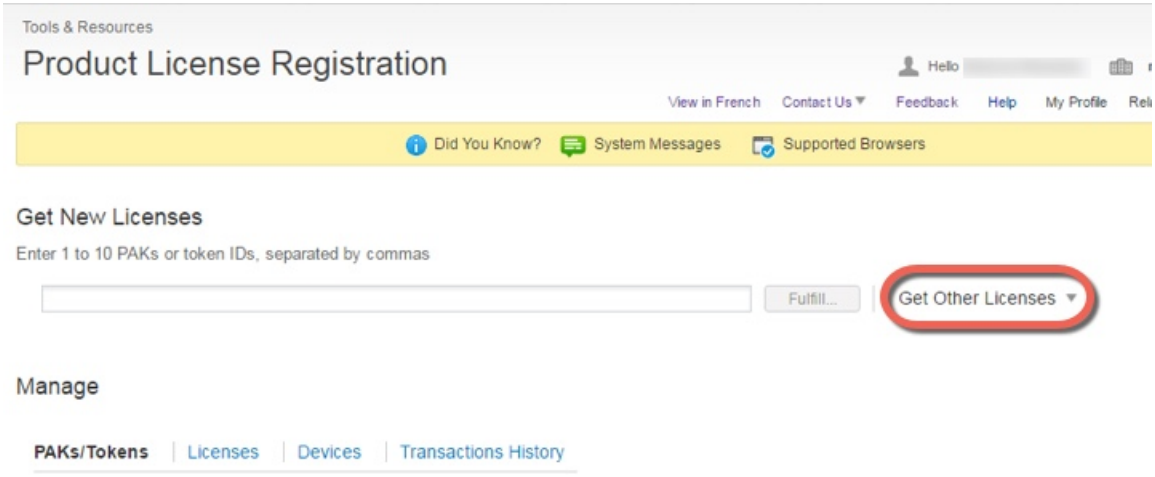
Étape 1 Utilisez la commande suivante pour obtenir le numéro de série de votre ASA :

show version | grep Serial

Ce numéro de série est différent de celui du châssis indiqué à l'extérieur du matériel. Le numéro de série du châssis est utilisé pour l'assistance technique, mais pas pour les licences.

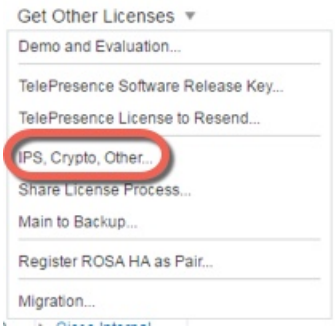
Étape 2 Consultez https://www.cisco.com/go/license, puis cliquez sur **Get Other Licenses** (Obtenir d'autres licences).

Illustration 2 : Get Other Licenses (obtenir d'autres licences)



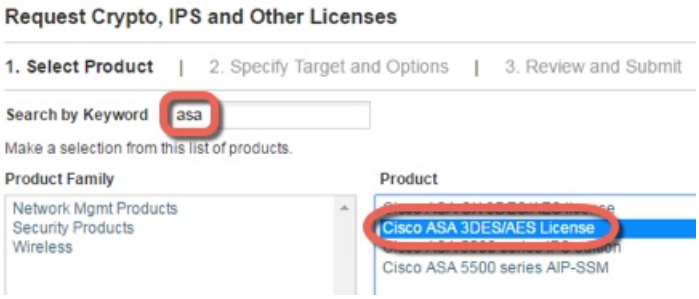
Étape 3 Choisissez **IPS, Crypto, Other**.

Illustration 3 : IPS, Crypto, Othe (IPS, cryptage, autre)



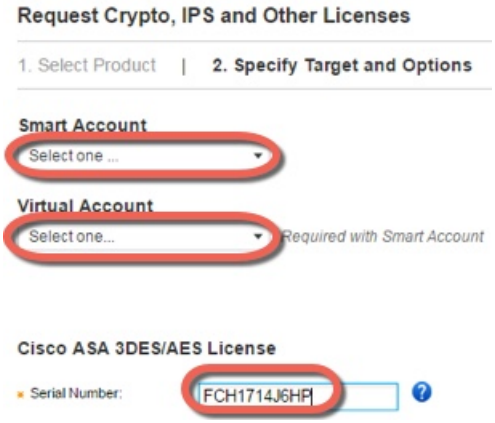
Étape 4 Dans le champ de recherche par mot clé **Search by Keyword** (Rechercher par mot clé), entrez **asa** et sélectionnez **Cisco ASA 3DES/AES License** (Licence Cisco ASA 3DES/AES).

Illustration 4 : Licence Cisco ASA 3DES/AES



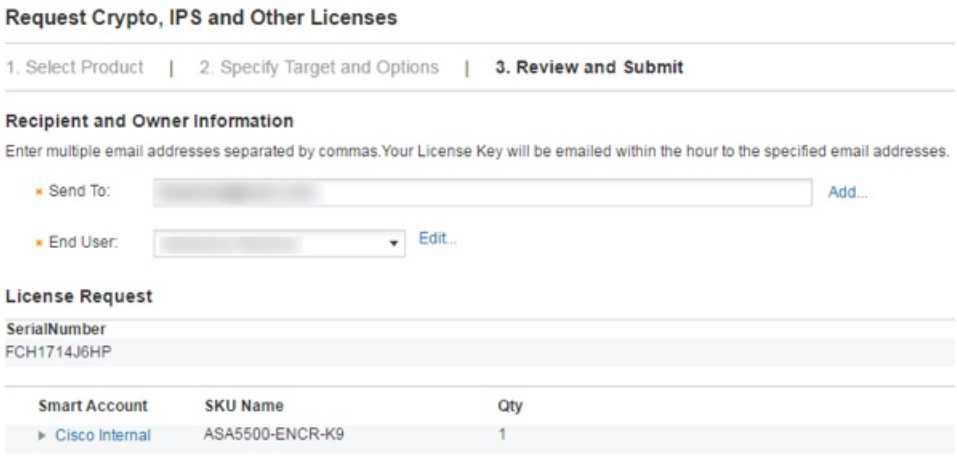
Étape 5 Sélectionnez votre **Smart Account** (Compte Smart) et votre **Virtual Account** (Compte virtuel), entrez le **Serial Number** (Numéro de série) de l'ASA, puis cliquez sur **Next** (Suivant) pour passer à l'étape suivante.

Illustration 5 : Smart Account (Compte Smart), Virtual Account (Compte virtuel) et Serial Number (Numéro de série)



Étape 6 L'adresse courriel du destinataire et le nom de l'utilisateur final sont automatiquement remplis. Si nécessaire, entrez les autres adresses courriel requises. Cochez la case **I Agree** (J'accepte) pour indiquer votre accord, puis cliquez sur **Submit** (Envoyer) pour envoyer le tout.

Illustration 6 : Submit (envoyer)



Étape 7 Vous recevrez alors un courriel contenant la clé d'activation, mais vous pouvez aussi la télécharger immédiatement depuis la zone de gestion des licences **Manage (Gérer)** > **Licenses (Licences)**.

Étape 8 Appliquez la clé d'activation conformément à Activer ou désactiver les clés, à la page 61.

Activer ou désactiver les clés

Cette section décrit comment saisir une nouvelle clé d'activation et comment activer et désactiver les clés à durée déterminée.

Avant de commencer

- Si vous êtes déjà en mode de contexte multiple, entrez la clé d'activation dans l'espace d'exécution du système.
- Certaines licences permanentes nécessitent que vous rechargiez l'ASA après les avoir activées. Le tableau suivant répertorie les licences qui nécessitent un rechargement.

Tableau 2 : Exigences en matière de rechargement de la licence permanente

Modèle	Action de licence nécessitant un rechargement
Tous les modèles	Rétrogradation de la licence de chiffrement.

Procédure

Étape 1 Appliquez une clé d'activation sur l'ASA :

activation-key *key* [**activate** | **deactivate**]

Exemple :

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

La *clé* est une chaîne hexadécimale de cinq éléments avec un espace entre chaque élément. Le spécificateur 0x de début est facultatif; toutes les valeurs sont censées être hexadécimales.

Vous pouvez installer une clé permanente et plusieurs clés à durée déterminée. Si vous entrez une nouvelle clé permanente, celle-ci remplacera la clé déjà installée.

Les mots clés **activate** et **deactivate** ne sont disponibles que pour les clés à durée déterminée. Si vous ne saisissez aucune valeur, **activate** est la valeur par défaut. La dernière clé à durée déterminée que vous activez pour une fonctionnalité donnée est la clé active. Pour désactiver une clé à durée déterminée active, saisissez le mot clé **deactivate**. Si vous saisissez une clé pour la première fois et indiquez **deactivate**, la clé est installée sur l'ASA à l'état inactif.

Étape 2 (Peut être nécessaire.) Rechargez l'ASA :

reload

Certaines licences permanentes nécessitent que vous rechargiez l'ASA après avoir saisi la nouvelle clé d'activation. Si vous devez le recharger, le message suivant s'affiche :

```
WARNING: The running activation key was not updated with the requested key.
The flash activation key was updated with the requested key, and will become
active after the next reload.
```

Sujets connexes

Licences à durée limitée, à la page 48

Configurer une licence partagée (Secure Client (services client sécurisés) 3 et versions antérieures)

Remarque La fonctionnalité de licence partagée sur l'ASA n'est pas prise en charge avec les licences Secure Client (services client sécurisés) 4 et ultérieures. Les licences Secure Client (services client sécurisés) sont partagées et ne nécessitent plus de serveur partagé ni de licence de participant.

Cette section décrit comment configurer le serveur de licences partagées et les participants.

À propos des licences partagées

Une licence partagée vous permet d'acheter un grand nombre de sessions Secure Client (services client sécurisés) Premium et de partager les sessions, selon les besoins, entre un groupe d'ASA en configurant l'un des ASA en tant que serveur de licences partagées et les autres en tant que participants aux licences partagées.

À propos du serveur de licences partagées et des participants

Les étapes suivantes décrivent le fonctionnement des licences partagées :

1. Décidez quel ASA doit être le serveur de licences partagées et achetez la licence de serveur de licences partagées en utilisant ce numéro de série de périphérique.
2. Décidez quels ASA doivent être des participants à une licence partagée, y compris le serveur de sauvegarde à licence partagée, et obtenez une licence de participant à une licence partagée pour chaque périphérique, en utilisant le numéro de série de chaque périphérique.
3. (Facultatif) Désignez un deuxième ASA comme serveur de sauvegarde de licences partagées. Vous ne pouvez définir qu'un seul serveur de sauvegarde.



Remarque Le serveur de sauvegarde de licences partagées n'a besoin que d'une licence de participant.

4. Configurez un secret partagé sur le serveur de licences partagées; tous les participants ayant le secret partagé peuvent utiliser la licence partagée.
5. Lorsque vous configurez l'ASA en tant que participant, il s'enregistre auprès du serveur de licences partagées en envoyant des renseignements sur lui-même, y compris la licence locale et les renseignements sur le modèle.



Remarque Le participant doit pouvoir communiquer avec le serveur sur le réseau IP; il ne doit pas être sur le même sous-réseau.

6. Le serveur de licences partagées répond par des renseignements sur la fréquence à laquelle le participant doit interroger le serveur.
7. Lorsqu'un participant utilise les sessions de la licence locale, il envoie une demande au serveur de licences partagées pour des sessions supplémentaires par incréments de 50 sessions.
8. Le serveur de licences partagées répond par une licence partagée. Le nombre total de sessions utilisées par un participant ne peut pas dépasser le nombre maximal de sessions pour le modèle de plateforme.



Remarque Le serveur de licences partagées peut également participer au regroupement de licences partagées. Il n'a pas besoin de licence de participant et de licence de serveur pour y participer.

   1. S'il ne reste pas assez de sessions dans le groupe de licences partagées pour le participant, le serveur répond par autant de sessions que disponible.
   2. Le participant continue d'envoyer des messages d'actualisation pour demander plus de sessions jusqu'à ce que le serveur puisse répondre de manière adéquate à la demande.

9. Lorsque la charge est réduite sur un participant, il envoie un message au serveur pour libérer les sessions partagées.



Remarque L'ASA utilise le protocole SSL entre le serveur et le participant pour chiffrer toutes les communications.

Problèmes de communication entre le participant et le serveur

Consultez les lignes directrices suivantes pour résoudre les problèmes de communication entre le participant et le serveur :

- Si un participant ne parvient pas à envoyer une actualisation après trois fois l'intervalle d'actualisation, le serveur libère les sessions dans le groupe de licences partagées.
- Si le participant ne parvient pas à atteindre le serveur de licences pour envoyer l'actualisation, il peut continuer à utiliser la licence partagée qu'il a reçue du serveur pendant un délai de 24 heures.
- Si le participant n'est toujours pas en mesure de communiquer avec un serveur de licences après 24 heures, le participant libère la licence partagée, même s'il a toujours besoin des sessions. Le participant laisse les connexions existantes établies, mais ne peut pas accepter de nouvelles connexions au-delà de la limite de licence.
- Si un participant se reconnecte au serveur avant l'expiration du délai de 24 heures, mais après l'expiration des sessions du participant par le serveur, le participant doit envoyer une nouvelle demande pour les sessions; le serveur répond avec autant de sessions que possible pouvant être réattribuées à ce participant.

À propos du serveur de sauvegarde de licences partagées

Le serveur de sauvegarde de licences partagées doit s'enregistrer auprès du serveur de licences partagées principal avant de pouvoir assumer son rôle de sauvegarde. Lors de l'enregistrement, le serveur de licences partagées principal synchronise les paramètres de serveur ainsi que les renseignements de licence partagée avec la sauvegarde, y compris une liste des participants inscrits et l'utilisation actuelle des licences. Le serveur principal et le serveur de sauvegarde synchronisent les données à des intervalles de 10 secondes. Après la synchronisation initiale, le serveur de sauvegarde peut effectuer des tâches de sauvegarde avec succès, même après un rechargement.

Lorsque le serveur principal tombe en panne, le serveur de sauvegarde prend le relais du fonctionnement du serveur. Le serveur de sauvegarde peut fonctionner jusqu'à 30 jours consécutifs, après quoi serveur de sauvegarde arrête d'émettre des sessions aux participants et les sessions existantes expirent. Assurez-vous de réinitialiser le serveur principal dans ce délai de 30 jours. Les messages de journal système de niveau critique sont envoyés à 15 jours et à nouveau à 30 jours.

Lorsque le serveur principal est remis en service, il se synchronise avec le serveur de sauvegarde, puis prend le relais du fonctionnement du serveur.

Lorsque le serveur de sauvegarde n'est pas actif, il agit comme un participant régulier du serveur de licences partagées principal.

Remarque Lorsque vous lancez le serveur de licences partagées principal pour la première fois, le serveur de sauvegarde ne peut fonctionner indépendamment que pendant 5 jours. La limite opérationnelle augmente de jour en jour jusqu'à 30 jours. De plus, si le serveur principal tombe en panne ultérieurement, la limite opérationnelle du serveur de sauvegarde diminuera de jour en jour. Lorsque le serveur principal est remis en service, le serveur de sauvegarde recommence à augmenter de jour en jour. Par exemple, si le serveur principal est en panne pendant 20 jours et que le serveur de sauvegarde est actif pendant ce temps, le serveur de sauvegarde n'aura plus qu'une limite de 10 jours. Le serveur de sauvegarde se « recharge » jusqu'à 30 jours après 20 jours supplémentaires en tant que sauvegarde inactive. Cette fonction de rechargement est mise en œuvre pour décourager toute utilisation abusive de la licence partagée.

Licences de basculement et partagées

Cette section décrit comment les licences partagées interagissent avec le basculement.

Serveurs de licences de basculement et partagées

Cette section décrit comment le serveur principal et le serveur de sauvegarde interagissent avec le basculement. Étant donné que le serveur de licences partagées remplit également les fonctions normales de l'ASA, notamment celles de passerelle VPN et de pare-feu, il peut être nécessaire de configurer le basculement pour les serveurs de licences partagés principal et de secours afin d'améliorer la fiabilité.



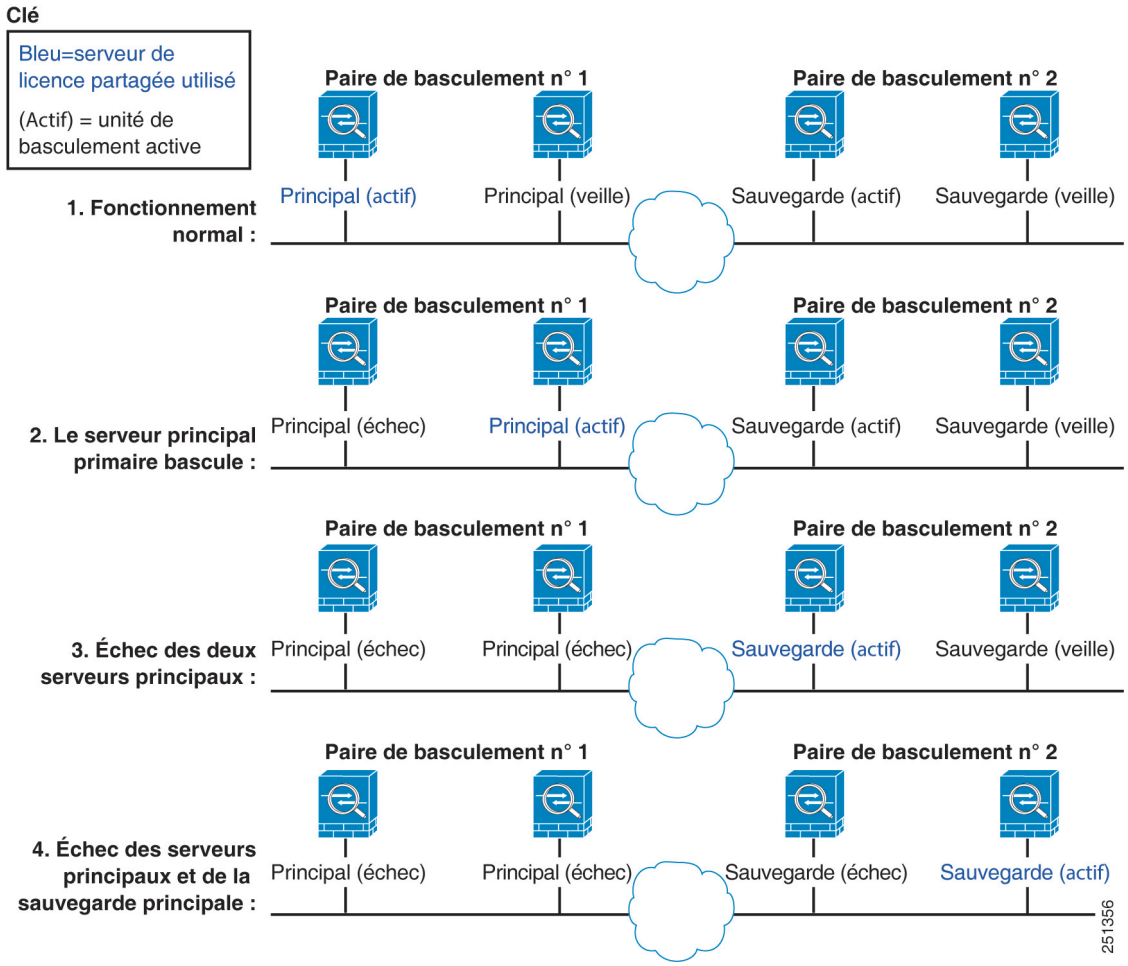
Remarque Le mécanisme du serveur de sauvegarde est distinct du basculement, mais compatible avec celui-ci.

Les licences partagées ne sont prises en charge qu'en mode de contexte unique, de sorte que le basculement actif/actif n'est pas pris en charge.

Pour le basculement actif/veille, l'unité principale agit en tant que serveur de licences partagées principal et l'unité de secours agit en tant que serveur de licences partagées principal après le basculement. L'unité de secours ne sert *pas* de serveur de licences partagées de secours. Au lieu de cela, vous pouvez avoir une deuxième paire d'unités agissant en tant que serveur de sauvegarde, si vous le souhaitez.

Par exemple, vous avez un réseau avec 2 paires de basculement. La paire n° 1 comprend le serveur de licences principal. La paire n° 2 comprend le serveur de sauvegarde. Lorsque l'unité principale de la paire n° 1 tombe en panne, l'unité en veille devient immédiatement le nouveau serveur de licences principal. Le serveur de sauvegarde de la paire n° 2 n'est jamais utilisé. Ce n'est que si les deux unités de la paire n° 1 tombent en panne que le serveur de sauvegarde de la paire n° 2 est utilisé comme serveur de licences partagées. Si la paire n° 1 reste en panne et que l'unité principale de la paire n° 2 tombe en panne, l'unité en veille de la paire n° 2 sert de serveur de licences partagées (voir la figure suivante).

Illustration 7 : Serveurs de licences de basculement et partagées



Le serveur de sauvegarde de secours partage les mêmes limites opérationnelles que le serveur de sauvegarde principal; si l'unité en veille devient active, elle continue le compte à rebours là où l'unité principale s'est arrêtée.

Sujets connexes

À propos du serveur de sauvegarde de licences partagées, à la page 64

Participants aux licences de basculement et partagées

Pour les paires de participants, les deux unités s'enregistrent auprès du serveur de licences partagées en utilisant des ID de participant distincts. L'unité active synchronise son ID de participant avec l'unité de sauvegarde. L'unité de sauvegarde utilise cet ID pour générer une demande de transfert lorsqu'elle passe au rôle actif. Cette demande de transfert est utilisée pour déplacer les sessions partagées de l'unité précédemment active vers la nouvelle unité active.

Nombre maximum de participants

L'ASA ne limite pas le nombre de participants pour la licence partagée; cependant, un très grand réseau partagé peut potentiellement affecter les performances du serveur de licences. Dans ce cas, vous pouvez augmenter le délai entre les actualisations des participants ou créer deux réseaux partagés.

Configurer le serveur de licences partagées

Cette section décrit comment configurer l'ASA pour qu'il soit un serveur de licences partagées.

Avant de commencer

Le serveur doit avoir une clé de serveur de licences partagées.

Procédure

Étape 1 Définissez le secret partagé :

license-server secret *secret*

Exemple :

```
ciscoasa(config)# license-server secret farscape
```

Le *secret* est une chaîne comprenant de 4 à 128 caractères ASCII. Tout participant ayant ce secret peut utiliser le serveur de licences.

Étape 2 (Facultatif) Définissez l'intervalle d'actualisation :

license-server refresh-interval *seconds*

Exemple :

```
ciscoasa(config)# license-server refresh-interval 100
```

L'intervalle est compris entre 10 et 300 secondes; cette valeur est fournie aux participants pour définir la fréquence à laquelle ils doivent communiquer avec le serveur. La valeur par défaut est de 30 secondes.

Étape 3 (Facultatif) Définissez le port sur lequel le serveur écoute les connexions SSL des participants :

license-server port *port*

Exemple :

```
ciscoasa(config)# license-server port 40000
```

Le *port* est compris entre 1 et 65 535. La valeur par défaut est le port TCP 50554.

Étape 4 (Facultatif) Déterminez l'adresse IP et le numéro de série du serveur de sauvegarde :

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

Exemple :

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

Si le serveur de sauvegarde fait partie d'une paire de basculement, identifiez également le numéro de série de l'unité de secours. Vous ne pouvez identifier qu'un seul serveur de sauvegarde et son unité de secours facultative.

Étape 5 Activez cette unité pour qu'elle soit le serveur de licences partagées :

license-server enable *interface_name*

Exemple :

```
ciscoasa(config)# license-server enable inside
```

Spécifiez l'interface sur laquelle les participants communiquent avec le serveur. Vous pouvez relancer cette commande pour autant d'interfaces que vous le souhaitez.

Exemples

L'exemple suivant définit le secret partagé, modifie l'intervalle d'actualisation et le port, configure un serveur de sauvegarde et active cette unité en tant que serveur de licences partagées sur l'interface interne et l'interface dmz :

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

Configurer le serveur de sauvegarde de licences partagées (facultatif)

Cette section permet à un participant à une licence partagée d'agir en tant que serveur de sauvegarde en cas de panne du serveur principal.

Avant de commencer

Le serveur de sauvegarde doit avoir une clé de participant à la licence partagée.

Procédure

Étape 1 Identifiez l'adresse IP du serveur de licences partagées et le secret partagé :

license-server address *address* **secret** *secret* [**port** *port*]

Exemple :

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

Si vous avez modifié le port par défaut dans la configuration du serveur, définissez le port du serveur de sauvegarde pour qu'il corresponde.

Étape 2 Activez cette unité pour qu'elle soit le serveur de sauvegarde de licences partagées :

license-server backup enable *interface_name*

Exemple :

```
ciscoasa(config)# license-server backup enable inside
```

Spécifiez l'interface sur laquelle les participants communiquent avec le serveur. Vous pouvez relancer cette commande pour autant d'interfaces que vous le souhaitez.

Exemples

L'exemple suivant identifie le serveur de licences et le secret partagé, et active cette unité en tant que serveur de sauvegarde de licences partagées sur l'interface interne et l'interface DMZ :

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

Configurer le participant à la licence partagée

Cette section configure un participant de licence partagée pour communiquer avec le serveur de licences partagées.

Avant de commencer

Le participant doit avoir une clé de participant à la licence partagée.

Procédure

Étape 1 Identifiez l'adresse IP du serveur de licences partagées et le secret partagé :

license-server address *address* **secret** *secret* [**port** *port*]

Exemple :

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

Si vous avez modifié le port par défaut dans la configuration du serveur, définissez le port du participant pour qu'il corresponde.

Étape 2 (Facultatif) Si vous avez configuré un serveur de sauvegarde, saisissez l'adresse du serveur de sauvegarde :

license-server backup address *address*

Exemple :

```
ciscoasa(config)# license-server backup address 10.1.1.2
```

Exemples

L'exemple suivant définit l'adresse IP et le secret partagé du serveur de licences, ainsi que l'adresse IP du serveur de licences de secours :

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

Licences de fonctionnalités prises en charge par modèle

Cette section décrit les licences disponibles pour chaque modèle et fournit des remarques importantes concernant les licences.

Licences par modèle

Cette section répertorie les licences de fonctionnalités disponibles pour chaque modèle :

Les éléments en *italique* sont des licences facultatives distinctes qui peuvent remplacer la version de licence de base (ou Security Plus, etc.). Vous pouvez combiner les licences facultatives.

Remarque Certaines fonctionnalités sont incompatibles entre elles. Consultez les chapitres consacrés aux différentes fonctionnalités pour obtenir des renseignements sur la compatibilité.

Si vous avez un modèle sans chiffrement des données utiles, certaines des fonctionnalités ci-dessous ne sont pas prises en charge. Consultez Aucun modèle de chiffrement des données utiles, à la page 54 pour obtenir la liste des fonctionnalités non prises en charge.

Pour de plus amples renseignements sur les licences, consultez Remarques relatives à la licence, à la page 50.

Fonctionnalités de la licence ISA 3000

Le tableau suivant présente les fonctionnalités sous licence pour l'ISA 3000.

Licences	Licence de base	Security Plus License
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune assistance	Aucune assistance
Connexions de pare-feu, simultanées	20 000	50 000

Licences	Licence de base		Security Plus License	
Carrier (exploitant)	Aucune assistance		Aucune assistance	
Nombre total de sessions de mandataire TLS	160		160	
Licences VPN				
Homologues Secure Client (services client sécurisés)	Désactivé	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement : 25 maximum*	Désactivé	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement : 25 maximum*
Autres homologues VPN	10		50	
Total des homologues VPN, tous types combinés	25		50	
Équilibrage de la charge VPN	Aucune assistance		Aucune assistance	
Licences générales				
Chiffrement	Base (DES)	*Licence opt. : renforcé (3DES/AES)*	Base (DES)	*Licence opt. : renforcé (3DES/AES)*
Basculement	Aucune assistance		Actif/Veille	
Contextes de sécurité	Aucune assistance		Aucune assistance	
Mise en grappe	Aucune assistance		Aucune assistance	
Nombre maximum de VLAN	5		25	

Supervision des licences PAK

Cette section décrit comment afficher les informations sur la licence.

Affichage de votre licence actuelle

Cette section décrit comment afficher votre licence actuelle et, pour les clés d'activation à durée limitée, le temps restant de la licence.

Avant de commencer

Si vous avez un modèle sans chiffrement des données utiles, vous affichez la licence, les licences VPN et de communications unifiées ne seront pas répertoriées. Consultez Aucun modèle de chiffrement des données utiles, à la page 54 pour de plus amples renseignements.

Procédure

Affichez la licence permanente, les licences actives à durée limitée et la licence en cours d'exécution, qui est une combinaison de la licence permanente et des licences actives à durée limitée :

show activation-key [**detail**]

Le mot clé **detail** affiche également les licences inactives à durée limitée.

Pour les unités de basculement ou de grappe, cette commande affiche également la licence de « grappe », qui regroupe les clés de toutes les unités.

Exemples

Exemple 1 : sortie de l'unité autonome pour la commande show activation-key

Voici un exemple de sortie de la commande **show activation-key** pour une unité autonome qui affiche la licence en cours d'exécution (les licences permanentes et les licences à durée limitée), ainsi que chaque licence active à durée limitée :

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
```

```
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

Exemple 2 : sortie de l'unité autonome pour la commande show activation-key detail

Voici un exemple de sortie de la commande **show activation-key detail** pour une unité autonome qui affiche la licence en cours d'exécution (les licences permanentes et les licences à durée limitée), ainsi que la licence permanente et chaque licence à durée limitée installée (active et inactive) :

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5512-X Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual
```

```
The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

Exemple 3 : sortie de l'unité principale dans une paire de basculement pour la commande show activation-key detail

Voici un exemple de sortie de la commande **show activation-key detail** pour l'unité de basculement principale qui affiche :

- La licence de l'unité principale (la licence permanente et les licences à durée déterminée combinées).
- La licence « grappe de basculement », qui regroupe les licences des unités principale et secondaire. Il s'agit de la licence qui est en cours d'exécution sur l'ASA. Les valeurs de cette licence qui reflètent la combinaison des licences principale et secondaire sont indiquées en gras.
- La licence permanente de l'unité principale.
- L'unité principale a installé des licences à durée limitée (actives et inactives).

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
```

```
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Active  perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Enabled        perpetual
Security Contexts             : 12             perpetual
GTP/GPRS                      : Enabled        perpetual
AnyConnect Premium Peers      : 4            perpetual
AnyConnect Essentials           : Disabled       perpetual
Other VPN Peers                 : 750            perpetual
Total VPN Peers                 : 750            perpetual
Shared License                  : Disabled       perpetual
AnyConnect for Mobile           : Disabled       perpetual
AnyConnect for Cisco VPN Phone  : Disabled       perpetual
Advanced Endpoint Assessment    : Disabled       perpetual
UC Phone Proxy Sessions       : 4              perpetual
Total UC Proxy Sessions       : 4              perpetual
Botnet Traffic Filter         : Enabled        33 days
Intercompany Media Engine     : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces   : Unlimited      perpetual
Maximum VLANs                 : 150            perpetual
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Active  perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Disabled       perpetual
Security Contexts             : 2              perpetual
GTP/GPRS                      : Disabled       perpetual
AnyConnect Premium Peers        : 2              perpetual
AnyConnect Essentials           : Disabled       perpetual
Other VPN Peers                 : 750            perpetual
Total VPN Peers                 : 750            perpetual
Shared License                  : Disabled        perpetual
AnyConnect for Mobile           : Disabled       perpetual
AnyConnect for Cisco VPN Phone  : Disabled       perpetual
Advanced Endpoint Assessment    : Disabled       perpetual
UC Phone Proxy Sessions       : 2              perpetual
Total UC Proxy Sessions       : 2              perpetual
Botnet Traffic Filter         : Disabled       perpetual
Intercompany Media Engine     : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter          : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts              : 2          7 days
AnyConnect Premium Peers                  : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions        : 100        14 days
```

Exemple 4 : sortie de l'unité secondaire dans une paire de basculement pour la commande show activation-key detail

Voici un exemple de sortie de la commande **show activation-key detail** pour l'unité de basculement secondaire qui affiche :

- La licence de l'unité secondaire (la licence permanente et les licences à durée déterminée combinées).
- La licence « grappe de basculement », qui regroupe les licences des unités principale et secondaire. Il s'agit de la licence qui est en cours d'exécution sur l'ASA. Les valeurs de cette licence qui reflètent la combinaison des licences principale et secondaire sont indiquées en gras.
- La licence permanente de l'unité secondaire.
- Les licences secondaires installées à durée limitée (actives et inactives). Cette unité n'a pas de licences à durée limitée, donc aucune n'est affichée dans cet exemple de sortie.

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
```

```
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

Exemple 5 : sortie de l'unité principale pour le module de services ASA dans une paire de basculement pour la commande show activation-key

Voici un exemple de sortie de la commande **show activation-key** pour l'unité de basculement principale qui affiche :

- La licence de l'unité principale (la licence permanente et les licences à durée déterminée combinées).
- La licence « grappe de basculement », qui regroupe les licences des unités principale et secondaire. Il s'agit de la licence qui est en cours d'exécution sur l'ASA. Les valeurs de cette licence qui reflètent la combinaison des licences principale et secondaire sont indiquées en gras.
- L'unité principale a installé des licences à durée limitée (actives et inactives).

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
```

```
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50 perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

Exemple 6 : sortie de l'unité secondaire pour le module de services ASA dans une paire de basculement pour la commande show activation-key

Voici un exemple de sortie de la commande **show activation-key** pour l'unité de basculement secondaire qui affiche :

- La licence de l'unité secondaire (la licence permanente et les licences à durée déterminée combinées).
- La licence « grappe de basculement », qui regroupe les licences des unités principale et secondaire. Il s'agit de la licence qui est en cours d'exécution sur l'ASA. Les valeurs de cette licence qui reflètent la combinaison des licences principale et secondaire sont indiquées en gras.
- Les licences secondaires installées à durée limitée (actives et inactives). Cette unité n'a pas de licences à durée limitée, donc aucune n'est affichée dans cet exemple de sortie.

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
```

```
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50 perpetual
GTP/GPRS                          : Enabled perpetual
Botnet Traffic Filter             : Enabled 330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

Exemple 7 : sortie dans une grappe pour la commande show activation-key

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual
```

```
This platform has an ASA 5585-X base license.

The flash permanent activation key is the SAME as the running permanent key.
```

Supervision de la licence partagée

Pour superviser la licence partagée, et saisissez l'une des commandes suivantes.

- **show shared license** [**detail** | **client** [*hostname*] | **backup**]

  Affiche les statistiques de licences partagées. Les mots clés facultatifs ne sont disponibles que pour le serveur de licences : le mot clé **detail** affiche les statistiques par participant. Pour limiter l'affichage à un participant, utilisez le mot clé **client**. Le mot clé **backup** affiche des renseignements sur le serveur de sauvegarde.

  Pour effacer les statistiques de licences partagées, saisissez la commande **clear shared license**.

  Voici un exemple de sortie de la commande **show shared license** sur le participant à la licence :

```
ciscoasa>  show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

  Voici un exemple de sortie de la commande **show shared license detail** sur le serveur de licences :

```
ciscoasa>  show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
```

```
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0


Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

- **show activation-key**

  Affiche les licences installées sur l'ASA. La commande **show version** affiche également les renseignements de licence.

- **show vpn-sessiondb**

  Affiche les renseignements de licence concernant les sessions VPN.

Historique des licences PAK

Nom de la caractéristique	Versions de plateforme	Description
Augmentation du nombre de connexions et de VLAN	7.0(5)	Augmentation des limites suivantes : • Connexions de licence de base ASA 5510 de 32 000 à 50 000; réseaux VLAN de 0 à 10. • Connexions de licence ASA 5510 Security Plus de 64 000 à 130 000; réseaux VLAN de 10 à 25. • Connexions ASA 5520 de 130 000 à 280 000; réseaux VLAN de 25 à 100. • Connexions ASA 5540 de 280 000 à 400 000; réseaux VLAN de 100 à 200.
Licences SSL VPN	7.1(1)	Des licences SSL VPN ont été introduites.
Augmentation du nombre de licences SSL VPN	7.2(1)	Une licence SSL VPN de 5 000 utilisateurs a été introduite pour les ASA 5550 et versions ultérieures.

Nom de la caractéristique	Versions de plateforme	Description
Augmentation du nombre d'interfaces pour la licence de base sur l'ASA 5510	7.2(2)	Pour la licence de base sur l'ASA 5510, le nombre maximum d'interfaces est passé de 3 plus une interface de gestion à un nombre illimité d'interfaces.
Augmentation du nombre de VLAN	7.2(2)	Le nombre maximum de VLAN pour la licence Security Plus sur l'ASA 5505 est passé de 5 (3 entièrement fonctionnels; 1 de basculement; un limité à une interface de secours) à 20 interfaces entièrement fonctionnelles. De plus, le nombre de ports de liaison est passé de 1 à 8. Il existe maintenant 20 interfaces entièrement fonctionnelles. Vous n'avez pas besoin d'utiliser la commande d'interface de sauvegarde pour chiffrer une interface ISP de secours; vous pouvez utiliser une interface entièrement fonctionnelle à cette fin. La commande d'interface de sauvegarde est toujours utile pour une configuration Easy VPN. Les limites de VLAN ont également été augmentées pour l'ASA 5510 (de 10 à 50 pour la licence de base et de 25 à 100 pour la licence Security Plus), l'ASA 5520 (de 100 à 150), l'ASA 5550 (de 200 à 250).
Prise en charge de Gigabit Ethernet pour la licence Security Plus sur l'ASA 5510	7.2(3)	L'ASA 5510 prend désormais en charge Gigabit Ethernet (1 000 Mbit/s) pour les ports Ethernet 0/0 et 0/1 avec la licence Security Plus. Dans la licence de base, ils continuent d'être utilisés comme ports Fast Ethernet (100 Mbit/s). Ethernet 0/2, 0/3 et 0/4 restent des ports Fast Ethernet pour les deux licences. **Remarque** Les noms d'interface restent Ethernet 0/0 et Ethernet 0/1. Utilisez la commande **speed** pour modifier la vitesse sur l'interface et utilisez la commande **show interface** pour voir quelle vitesse est actuellement configurée pour chaque interface.

Nom de la caractéristique	Versions de plateforme	Description
Licence d'évaluation de point d'accès avancée	8.0(2)	Licence d'évaluation de point d'accès avancée a été introduite. Comme condition à l'achèvement d'une connexion Cisco AnyConnect ou d'une connexion SSL VPN sans client, l'ordinateur distant analyse une série considérablement élargie d'applications antivirus et anti-logiciel espion, de pare-feu, de systèmes d'exploitation et de mises à jour associées. Il analyse également les entrées de registre, les noms de fichiers et les noms de processus que vous spécifiez. Il envoie les résultats de l'analyse à l'ASA. L'ASA utilise les coordonnées de connexion de l'utilisateur et les résultats de l'analyse de l'ordinateur pour attribuer une politique d'accès dynamique (DAP). Avec une licence d'évaluation de point d'accès avancée, vous pouvez améliorer l'analyse de l'hôte en configurant une tentative de mise à jour des ordinateurs non conformes pour répondre aux exigences de la version. Cisco peut fournir des mises à jour en temps opportun de la liste des applications et des versions prises en charge par l'analyse de l'hôte dans un progiciel distinct de Cisco Secure Desktop.
Équilibrage de charges du VPN pour l'ASA 5510	8.0(2)	L'équilibrage de charges du VPN est désormais pris en charge sur la licence Security Plus de l'ASA 5510.
Licence AnyConnect pour mobile	8.0(3)	La licence AnyConnect pour mobile a été introduite. Elle permet aux périphériques mobiles Windows de se connecter à l'ASA à l'aide du Secure Client (services client sécurisés).
Licences à durée limitée	8.0(4)/8.1(2)	La prise en charge des licences à durée limitée a été introduite.
Augmentation du nombre de VLAN pour l'ASA 5580	8.1(2)	Le nombre de VLAN pris en charge sur l'ASA 5580 est passé de 100 à 250.
Licence de sessions de mandataire pour les communications unifiées	8.0(4)	La licence de sessions de mandataire UC a été introduite. Les applications de mandataire téléphonique, de mandataire de fédération de présence et d'inspection de voix chiffrée utilisent des sessions de mandataire TLS pour leurs connexions. Chaque session de mandataire TLS est prise en compte dans la limite de licences UC. Toutes ces applications sont sous licence dans le cadre de l'offre de mandataires UC, et peuvent être combinées entre elles. Cette fonctionnalité n'est pas disponible dans la version 8.1.
Licence de filtre de trafic de réseau de zombies	8.2(1)	La licence de filtre de trafic de réseau de zombies a été introduite. Le filtre de trafic de réseau de zombies protège contre les activités réseau de programmes malveillants en suivant les connexions aux domaines et aux adresses IP connus pour être malveillants.

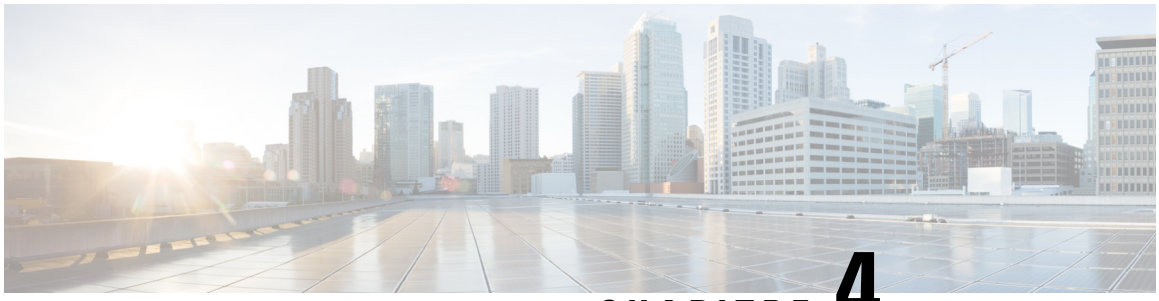
Nom de la caractéristique	Versions de plateforme	Description
Licence AnyConnect Essentials	8.2(1)	La licence AnyConnect Essentials a été introduite. Cette licence active l'accès client VPN AnyConnect à l'ASA. Cette licence ne prend pas en charge l'accès SSL VPN par navigateur ou Cisco Secure Desktop. Pour ces fonctionnalités, activez une licence AnyConnect Premium au lieu de la licence AnyConnect Essentials. **Remarque** Grâce à la licence AnyConnect Essentials, les utilisateurs de VPN peuvent utiliser un navigateur pour se connecter, télécharger et lancer (WebLaunch) le Secure Client (services client sécurisés). Le logiciel Secure Client (services client sécurisés) offre le même ensemble de fonctionnalités client, qu'il soit activé par cette licence ou une licence AnyConnect Premium. La licence AnyConnect Essentials ne peut pas être active en même temps que les licences suivantes sur un ASA donné : licence AnyConnect Premium (tous les types) ou licence d'évaluation de point d'accès avancée. Vous pouvez toutefois exécuter les licences AnyConnect Essentials et AnyConnect Premium sur différents ASA dans le même réseau. Par défaut, l'ASA utilise la licence AnyConnect Essentials, mais vous pouvez la désactiver pour utiliser d'autres licences en utilisant l'argument **webvpn**, puis la commande **no anyconnect-essentials**.
Licence SSL VPN remplacée par une licence AnyConnect Premium SSL VPN Edition	8.2(1)	Le nom de la licence SSL VPN a été remplacé par la licence AnyConnect Premium SSL VPN Edition.
Licences partagées pour SSL VPN	8.2(1)	Des licences partagées pour SSL VPN ont été introduites. Plusieurs ASA peuvent partager un ensemble de sessions SSL VPN selon les besoins.
L'application du mandataire de mobilité ne nécessite plus de licence de mandataire de connexions unifiées	8.2(2)	Le mandataire de mobilité ne nécessite plus la licence de mandataire UC.
Licence d'E/S 10 GE pour l'ASA 5585-X avec SSP-20	8.2(3)	Nous avons introduit la licence d'E/S 10 GE pour l'ASA 5585-X avec SSP-20 afin de permettre des vitesses de 10 Gigabit Ethernet pour les ports de fibre optique. Le SSP-60 prend en charge des vitesses de 10 Gigabit Ethernet par défaut. **Remarque** L'ASA 5585-X n'est pas pris en charge dans la version 8.3(x).

Nom de la caractéristique	Versions de plateforme	Description
Licence d'E/S 10 GE pour l'ASA 5585-X avec SSP-10	8.2(4)	Nous avons introduit la licence d'E/S 10 GE pour l'ASA 5585-X avec SSP-10 afin de permettre des vitesses de 10 Gigabit Ethernet pour les ports de fibre optique. Le SSP-40 prend en charge des vitesses de 10 Gigabit Ethernet par défaut. **Remarque** L'ASA 5585-X n'est pas pris en charge dans la version 8.3(x).
Licences de basculement non identiques	8.3(1)	Les licences de basculement n'ont plus besoin d'être identiques sur chaque unité. La licence utilisée pour les deux unités est la licence combinée des unités principale et secondaire. Nous avons modifié les commandes suivantes : **show activation-key** et **show version**.
Licences empilables à durée limitée	8.3(1)	Les licences à durée limitée sont maintenant empilables. Dans de nombreux cas, vous devrez peut-être renouveler votre licence temporaire et effectuer une transition transparente de l'ancienne licence à la nouvelle. Pour les fonctionnalités qui ne sont disponibles qu'avec une licence à durée limitée, il est particulièrement important que la licence n'expire pas avant que vous puissiez appliquer la nouvelle licence. L'ASA vous permet d'*empiler* des licences à durée limitée afin que vous n'ayez pas à vous soucier de l'expiration de la licence ou de la perte de temps sur vos licences en raison de l'installation de la nouvelle licence plus tôt.
Licence Intercompany Media Engine	8.3(1)	La licence IME a été introduite.
Plusieurs licences à durée limitée actives en même temps	8.3(1)	Vous pouvez maintenant installer plusieurs licences à durée limitée et avoir une licence par fonctionnalité active à la fois. Nous avons modifié les commandes suivantes : **show activation-key** et **show version**.
Activation et désactivation discrétionnaires des licences à durée limitée.	8.3(1)	Vous pouvez maintenant activer ou désactiver des licences à durée limitée à l'aide d'une commande. Nous avons modifié les commandes suivantes : **activation-key** [**activate** | **deactivate**].
Licence AnyConnect Premium SSL VPN Edition remplacée par une licence AnyConnect Premium SSL VPN	8.3(1)	Le nom de la licence AnyConnect Premium SSL VPN Edition a été remplacé par la licence AnyConnect Premium SSL VPN.

Nom de la caractéristique	Versions de plateforme	Description
Aucune image de chiffrement des données utiles à exporter	8.3(2)	Si vous installez le logiciel sans chiffrement des données utiles sur les ASA 5505 à 5550, vous désactiverez les communications unifiées, le VPN de cryptage renforcé et les protocoles de gestion de cryptage renforcé. **Remarque** Cette image spéciale n'est prise en charge que dans 8.3(x); pour la prise en charge du chiffrement des données utiles dans les versions 8.4(1) et ultérieures, vous devez acheter une version matérielle spéciale de l'ASA.
Augmentation du nombre de contextes pour les ASA 5550, 5580 et 5585-X	v 8.4(1)	Pour les ASA 5550 et ASA 5585-X avec SSP-10, le nombre maximum de contextes est passé de 50 à 100. Pour les ASA 5580 et 5585-X avec SSP-20 et versions ultérieures, le maximum est passé de 50 à 250.
Augmentation du nombre de VLAN pour les ASA 5580 et 5585-X	v 8.4(1)	Pour les ASA 5580 et 5585-X, le nombre maximum de VLAN est passé de 250 à 1 024.
Augmentation du nombre de connexions pour les ASA 5580 et 5585-X	v 8.4(1)	Nous avons augmenté les limites de connexion du pare-feu : • ASA 5580-20 : 1 000 000 à 2 000 000. • ASA 5580-40 : 2 000 000 à 4 000 000. • ASA 5585-X avec SSP-10 : 750 000 à 1 000 000. • ASA 5585-X avec SSP-20 : 1 000 000 à 2 000 000. • ASA 5585-X avec SSP-40 : 2 000 000 à 4 000 000. • ASA 5585-X avec SSP-60 : 2 000 000 à 10 000 000.
Licence AnyConnect Premium SSL VPN remplacée par la licence AnyConnect Premium	v 8.4(1)	Le nom de la licence AnyConnect Premium SSL VPN a été remplacé par la licence AnyConnect Premium. L'affichage des renseignements sur la licence est passé de « SSL VPN Peers » (Homologues SSL VPN) à « AnyConnect Premium Peers » (Homologues AnyConnect Premium).
Augmentation du nombre de sessions VPN AnyConnect pour l'ASA 5580	v 8.4(1)	La limite de sessions VPN AnyConnect est passée de 5 000 à 10 000.
Augmentation du nombre de sessions Autre VPN pour l'ASA 5580	v 8.4(1)	La limite de sessions Autre VPN est passée de 5 000 à 10 000.

Nom de la caractéristique	Versions de plateforme	Description
VPN d'accès à distance IPsec avec IKEv2	v 8.4(1)	Le VPN d'accès à distance IPsec avec IKEv2 a été ajouté aux licences AnyConnect Essentials et AnyConnect Premium. **Remarque** La limite suivante existe dans notre prise en charge de IKEv2 sur l'ASA : nous ne prenons actuellement pas en charge les associations de sécurité en double. Les sessions de site à site IKEv2 ont été ajoutées à la licence Autre VPN (anciennement VPN IPsec). La licence Autre VPN est incluse dans la licence de base.
Aucun matériel de chiffrement des données utiles à exporter	v 8.4(1)	Pour les modèles disponibles sans chiffrement des données utiles (par exemple, l'ASA 5585-X), le logiciel ASA désactive les communications unifiées et les fonctions VPN, ce qui rend l'ASA disponible pour l'exportation vers certains pays.
Doubles SSP pour SSP-20 et SSP-40	8.4(2)	Pour SSP-40 et SSP-60, vous pouvez utiliser deux SSP de même niveau dans le même châssis. Les SSP de niveau mixte ne sont pas pris en charge (par exemple, un SSP-40 avec un SSP-60 n'est pas pris en charge). Chaque SSP agit en tant qu'appareil indépendant, avec des configurations et une gestion distinctes. Vous pouvez utiliser les deux SSP comme paire de basculement si vous le souhaitez. Lors de l'utilisation de deux SSP dans le châssis, le VPN n'est pas pris en charge; notez, cependant, que le VPN n'a pas été désactivé.
Licence de module IPS pour les modèles ASA 5512-X à ASA 5555-X	8.6(1)	Le module logiciel IPS SSP sur les modèles ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X et ASA 5555-X nécessite la licence de module IPS.
Licence de mise en grappe pour les modèles ASA 5580 et ASA 5585-X.	9.0(1)	Une licence de mise en grappe a été ajoutée pour les modèles ASA 5580 et ASA 5585-X.
Prise en charge du VPN sur l'ASASM	9.0(1)	L'ASASM prend désormais en charge toutes les fonctionnalités VPN.
Prise en charge des communications unifiées sur l'ASASM	9.0(1)	L'ASASM prend désormais en charge toutes les fonctionnalités de communications unifiées.
Prise en charge du double SSP ASA 5585-X pour les SSP-10 et SSP-20 (en plus de SSP-40 et SSP-60); prise en charge du VPN pour les doubles SSP	9.0(1)	L'ASA 5585-X prend désormais en charge les doubles SSP utilisant tous les modèles SSP (vous pouvez utiliser deux SSP de même niveau dans le même châssis). Le VPN est désormais pris en charge lors de l'utilisation de deux SSP.
Prise en charge de l'ASA 5500-X pour la mise en grappe	9.1(4)	Les modèles ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X et ASA 5555-X prennent désormais en charge les grappes de deux unités. La mise en grappe pour 2 unités est activée par défaut dans la licence de base; pour l'ASA 5512-X, vous avez besoin de la licence Security Plus.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de 16 membres d'une grappe pour l'ASA 5585-X	9.2(1)	L'ASA 5585-X prend désormais en charge les grappes de 16 unités.
Les licences des modèles ASAv4 et ASAv30 Standard et Premium ont été introduites	9.2(1)	L'ASAv a été introduit avec un schéma de licence simple : des licences permanentes ASAv4 et ASAv30 de niveau Standard ou Premium. Aucune licence complémentaire n'est disponible.



CHAPITRE 4

Licences : gestion des licences logicielles Smart

Smart Software Licensing vous permet d'acheter et de gérer un ensemble de licences de manière centralisée. Contrairement aux licences de clé d'autorisation de produit (PAK), les licences Smart ne sont pas liées à un numéro de série spécifique. Vous pouvez facilement déployer ou retirer des ASA sans avoir à gérer la clé de licence de chaque unité. Smart Software Licensing vous permet également de consulter votre utilisation et vos besoins en licences en un clin d'œil.

Remarque Smart Software Licensing n'est pas pris en charge sur ISA 3000. Ils utilisent des licences PAK. Consultez À propos des licences PAK, à la page 47.

Pour en savoir plus sur les fonctionnalités des licences Smart et les comportements par plateforme, consultez la section Gammes de produits compatibles avec les licences intelligentes.

- À propos des licences logicielles Smart, à la page 89
- Conditions préalables à la gestion de licences logicielles Smart, à la page 111
- Gestion des licences logicielles Smart, à la page 112
- Paramètres par défaut des licences logicielles Smart, à la page 113
- ASA virtuel : configurer les licences logicielles Smart, à la page 113
- 1000/2100/3100 : configurer les licences logicielles Smart, à la page 133
- Firepower 4100/9300 : configurer les licences logicielles Smart, à la page 146
- Licences par modèle, à la page 149
- PID de licence par modèle, à la page 161
- Supervision des licences logicielles Smart, à la page 165
- Communication avec Smart Software Manager, à la page 169
- Historique des licences logicielles Smart, à la page 171

À propos des licences logicielles Smart

Cisco Smart Licensing est un modèle de licence flexible qui vous offre un moyen plus facile, plus rapide et plus cohérent d'acheter et de gérer les logiciels du portefeuille Cisco et de votre organisme. De plus, il est sécurisé : vous contrôlez ce à quoi les utilisateurs peuvent accéder. Avec les licences Smart, vous obtenez :

- **Easy Activation** (Activation facile) : les licences Smart établissent un ensemble de licences logicielles qui peuvent être utilisées dans l'ensemble de l'entreprise. Plus de clés d'activation de produit (PAK).

- **Unified Management** (Gestion unifiée) : My Cisco Entitlements (MCE) fournit une vue complète de tous vos produits et services Cisco dans un portail facile à utiliser, afin que vous sachiez toujours ce que vous avez et ce que vous utilisez.
- **License Flexibility** (Flexibilité des licences) : votre logiciel n'est pas verrouillé par un nœud sur votre matériel, vous pouvez donc facilement utiliser et transférer des licences selon vos besoins.

Pour utiliser les licences Smart, vous devez d'abord configurer un compte Smart sur Cisco Software Central (software.cisco.com).

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

Licences logicielles Smart pour l'ASA sur le Châssis Firepower 4100/9300

Pour l'ASA sur le Châssis Firepower 4100/9300 , la configuration de la licence logicielle Smart est partagée entre le superviseur Châssis Firepower 4100/9300 et l'ASA.

- Châssis Firepower 4100/9300 : configurez toute l'infrastructure de licences logicielles Smart sur le châssis, y compris les paramètres de communication avec le Smart Software Manager. Le Châssis Firepower 4100/9300 lui-même ne nécessite aucune licence pour fonctionner. Consultez le guide de configuration FXOS pour connaître les procédures de licence.

Remarque La mise en grappe inter-châssis exige que vous activiez la même méthode de licence Smart sur chaque châssis de la grappe.

- Application ASA : configurez tous les droits de licence de l'ASA.

Gestionnaire de logiciels et comptes Smart

Lorsque vous achetez une ou plusieurs licences pour l'appareil, vous les gérez dans le Cisco Smart Software Manager :

https://software.cisco.com/#module/SmartLicensing

Smart Software Manager vous permet de créer un compte principal pour votre organisation.

Remarque Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.

Par défaut, vos licences sont affectées au *compte virtuel par défaut* sous votre compte maître. En tant qu'administrateur du compte, vous pouvez éventuellement créer des comptes virtuels supplémentaires; par exemple, vous pouvez créer des comptes pour des régions, les services ou les filiales. Plusieurs comptes virtuels vous permettent de gérer plus facilement un grand nombre de licences et de périphériques.

Gestion hors ligne

Si vos périphériques n'ont pas d'accès Internet et ne peuvent pas s'inscrire auprès du Smart Software Manager, vous devez configurer la licence hors ligne.

Réservation de licence permanente

Si vos périphériques ne peuvent pas accéder à Internet pour des raisons de sécurité, vous pouvez éventuellement demander des licences permanentes pour chaque ASA. Les licences permanentes ne nécessitent pas d'accès périodique à Smart Software Manager. Comme pour les licences PAK, vous pouvez acheter une licence et installer la clé de licence pour l'ASA. Contrairement à une licence PAK, vous pouvez obtenir et gérer les licences avec Smart Software Manager. Vous pouvez facilement passer du mode de licence Smart normal au mode de réservation de licence permanente.

Remarque L'ASA ne prend pas en charge la réservation d'une licence spécifique (SLR). Dans SLR, les droits de fonctionnalités spécifiques sont activés en permanence. L'ASA prend en charge uniquement le PLR, où toutes les fonctionnalités sont activées en permanence.

Réservation de licence permanente pour l'ASA virtuel

Remarque La réservation de licence permanente est prise en charge uniquement sur VMware et KVM.

Vous pouvez obtenir une licence spécifique au modèle qui active toutes les fonctionnalités suivantes :

- Débit maximal pour votre modèle
- Niveau Essentials
- Licence de cryptage renforcé (3DES et AES), si vous l'avez activée dans votre compte de licences Smart
- Fonctionnalités Secure Client (services client sécurisés) activées pour la plateforme

Remarque L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

Mode de réservation de licences permanentes en fonction de la mémoire et du vCPU

Vous pouvez configurer une licence spécifique au modèle en fonction de la RAM et des vCPU attribuées à votre ASA virtuel. Par exemple, un ASA virtuel avec 8 Go de RAM et 4 vCPU utilise toujours une licence ASAv30 avec un débit de 2 Go.

Les relations entre les vCPU et la mémoire à la licence sont les suivantes :

- 2 Go, 1 vCPU – ASAv5 (100 M) (Vous devez exécuter la commande **license smart set_plr5**; sinon, la licence ASAv10 est attribuée pour autoriser un débit de 1 Go.)

Remarque Dans la version 9.13, les exigences de RAM ASAv5 ont été augmentées à 2 Go. En raison de cette augmentation, la licence permanente ASAv5 ne fonctionnait plus, car l'ASA vérifiait la mémoire attribuée et déterminait que 2 Go de RAM correspondaient en réalité à une licence ASAv10, et non ASAv5. Pour permettre à la licence permanente ASAv5 de fonctionner, vous devez configurer l'ASA afin qu'il reconnaisse la mémoire supplémentaire pour le modèle.

- 2 Go, 1 vCPU – ASAv10 (1G)
- 8 Go, 4 vCPU – ASAv30 (2G)
- 16 Go, 8 vCPU – ASAv50 (10G)
- 32 Go, 16 vCPU – ASAv100 (20G)

Plus tard, si vous souhaitez modifier le niveau de modèle d'une unité, vous devrez renvoyer la licence actuelle et demander une nouvelle licence au niveau de modèle correct. Pour modifier le modèle d'un ASA virtuel déjà déployé, à partir de l'hyperviseur, vous pouvez modifier les paramètres des vCPU et de la DRAM pour qu'ils correspondent aux exigences du nouveau modèle. Consultez le *Guide de démarrage d'ASA virtuel virtuel* pour connaître ces valeurs.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA virtuel, puis saisir ce code dans Smart Software Manager. Vous devez suivre correctement le processus de retour pour vous assurer de ne pas payer pour les licences inutilisées.

Pour en savoir plus sur la configuration de la réservation de licence permanente, consultez ASA virtuel: configurer la réservation de licence permanente, à la page 128.

Réservation de licence permanente pour Firepower 1010

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Security Plus
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour Firepower 1100

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Nombre maximum de contextes de sécurité
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour Firepower 2100

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Nombre maximum de contextes de sécurité
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour Secure Firewall 3100

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials
- Nombre maximum de contextes de sécurité
- Licence d'opérateur
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

Remarque Vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'ASA, puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Réservation de licence permanente pour le châssis Firepower 4100/9300

Vous pouvez obtenir une licence qui active toutes les fonctionnalités :

- Niveau Essentials.
- Nombre maximum de contextes de sécurité
- Licence d'opérateur
- Licence de cryptage renforcé (3DES/AES) si votre compte est admissible
- Capacités Secure Client (services client sécurisés) activées au maximum de la plateforme.

  L'utilisation des fonctionnalités Secure Client (services client sécurisés) est conditionnelle à l'achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

Remarque La licence est gérée sur le Châssis Firepower 4100/9300 , mais vous devez également demander les droits dans la configuration ASA pour que celui-ci permette leur utilisation. Pour gérer la licence, consultez le Guide de configuration FXOS.

Si vous cessez d'utiliser une licence, vous devez renvoyer la licence en générant un code de retour sur l'Châssis Firepower 4100/9300 , puis en saisissant ce code dans Smart Software Manager. Assurez-vous de suivre correctement le processus de retour afin de ne pas payer pour des licences inutilisées.

Smart Software Manager sur place

Si vos périphériques ne peuvent pas accéder à Internet pour des raisons de sécurité, vous pouvez éventuellement installer un serveur Smart Software Manager sur site (anciennement appelé « serveur satelitte Smart Software ») local en tant que machine virtuelle (VM). Smart Software Manager sur site fournit un sous-ensemble des fonctionnalités de Smart Software Manager et vous permet de fournir des services de licence essentiels pour tous vos périphériques locaux. Seul Smart Software Manager sur site doit se connecter périodiquement au Smart Software Manager principal pour synchroniser votre utilisation des licences. Vous pouvez effectuer la synchronisation selon un calendrier défini ou manuellement.

Vous pouvez exécuter les fonctions suivantes sur Smart Software Manager sur site :

- Activer ou enregistrer une licence
- Afficher les licences de votre entreprise
- Transférer des licences entre les entités de l'entreprise

Pour en savoir plus, consultez la Fiche technique de Cisco Smart Software Manager sur site.

Licences et appareils gérés par compte virtuel

Les licences et les périphériques sont gérés par compte virtuel : seuls les périphériques de ce compte virtuel peuvent utiliser les licences attribuées au compte. Si vous avez besoin de licences supplémentaires, vous pouvez transférer une licence inutilisée d'un autre compte virtuel. Vous pouvez également transférer des périphériques entre des comptes virtuels.

Pour l'ASA sur le Châssis Firepower 4100/9300 :seul le châssis s'enregistre en tant que périphérique, tandis que les applications ASA dans le châssis demandent leurs propres licences. Par exemple, pour un châssis Firepower 9300 avec 3 modules de sécurité, le châssis compte comme un seul périphérique, mais les modules utilisent 3 licences distinctes.

Licence d'évaluation.

ASA virtuel

L'ASA virtuel ne prend pas en charge de mode d'évaluation. Avant que l'ASA virtuel ne s'enregistre avec Smart Software Manager, il fonctionne dans un état fortement limité en termes de débit.

Firepower 1000

Avant que le Firepower 1000 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. Seuls les droits par défaut sont activés. À la fin de cette période, le Firepower 1000 devient non conforme.



Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

Firepower de la série 2100

Avant que le Firepower 2100 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. Seuls les droits par défaut sont activés. À la fin de cette période, le Firepower 2100 devient non conforme.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

Cisco Secure Firewall 3100

Avant que le Secure Firewall 3100 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. Seuls les droits par défaut sont activés. À la fin de cette période, le Secure Firewall 3100 devient non conforme.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

Châssis Firepower 4100/9300

Le Châssis Firepower 4100/9300 prend en charge deux types de licence d'évaluation :

- Mode d'évaluation au niveau du châssis : avant que le Châssis Firepower 4100/9300 ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours (utilisation totale) en mode d'évaluation. L'ASA ne peut pas demander de droits spécifiques dans ce mode; seuls les droits par défaut sont activés. À la fin de cette période, le Châssis Firepower 4100/9300 devient non conforme.
- Mode d'évaluation basé sur les droits : après l'enregistrement de Châssis Firepower 4100/9300 auprès de Smart Software Manager, vous pouvez obtenir des licences d'évaluation à durée limitée qui peuvent être attribuées à l'ASA. Dans l'ASA, vous demandez des droits comme d'habitude. Lorsque la licence à durée limitée expire, vous devez soit renouveler la licence à durée limitée, soit obtenir une licence permanente.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le cryptage renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager et obtenir une licence permanente pour recevoir le jeton de conformité pour l'exportation qui active la licence de cryptage renforcé (3DES/AES).

À propos des licences par type

Les sections suivantes contiennent des renseignements supplémentaires sur les licences par type.

LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement

Les licences Secure Client (services client sécurisés) ne sont pas appliquées directement à l'ASA. Cependant, vous devez acheter des licences et les ajouter à votre compte Smart pour garantir le droit d'utiliser l'ASA comme tête de réseau Secure Client (services client sécurisés).

- Pour les licences Secure Client Advantage et Secure Client Premier, ajoutez le nombre d'homologues que vous envisagez d'utiliser pour tous les ASA de votre compte Smart et achetez des licences pour ce nombre d'homologues.
- Pour le VPN client sécurisé uniquement , achetez une licence par ASA. Contrairement aux autres licences qui fournissent un ensemble d'homologues pouvant être partagés par plusieurs ASA, la licence VPN client sécurisé uniquement est gérée par tête de réseau.

Pour obtenir plus de renseignements, consultez la section :

- Guide de commande Cisco Secure Client (services client sécurisés)
- Foire aux questions (FAQ) Secure Client (services client sécurisés) Licensing

Autres homologues VPN

Les autres homologues VPN comprennent les types de VPN suivants :

- VPN d'accès à distance IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv1
- VPN de site à site IPsec avec IKEv2

Cette licence est incluse dans la licence de base.

Total des homologues VPN combinés, tous types

- Le nombre total d'homologues VPN est le nombre maximum d'homologues VPN autorisés pour les homologues Secure Client (services client sécurisés) et autres homologues VPN combinés. Par exemple, si le total est de 1 000, vous pouvez autoriser 500 homologues Secure Client (services client sécurisés) et 500 autres homologues VPN simultanément; ou 700 homologues Secure Client (services client sécurisés) et 300 autres VPN; ou utiliser les 1 000 pour Secure Client (services client sécurisés). Si vous dépassez le nombre total d'homologues VPN, vous pouvez surcharger l'ASA. Assurez-vous donc de dimensionner votre réseau de manière appropriée.

Licence de chiffrement

Cryptage renforcé : ASA virtuel

Le cryptage renforcé (3DES/AES) est disponible pour les connexions de gestion avant de vous connecter au Smart Software Manager ou au serveur Smart Software Manager sur site afin que vous puissiez lancer ASDM et vous connecter au Smart Software Manager. Pour le trafic de transit qui nécessite un cryptage renforcé (comme VPN), le débit est fortement limité jusqu'à ce que vous vous connectiez à Smart Software Manager et obteniez la licence de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour l'ASA virtuel à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered**

with this token (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation). Si l'ASA virtuel devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA virtuel conservera la licence et ne reviendra pas à l'état de débit limité. La licence est supprimée si vous réenregistrez l'ASA virtuel et que la conformité à l'exportation est désactivée, ou si vous restaurez les paramètres d'usine par défaut de l'ASA virtuel.

Si vous enregistrez initialement l'ASA virtuel sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'ASA virtuel pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

Cryptage renforcé : Firepower 1000, Firepower 2100 en mode appareil, Secure Firewall 3100

L'ASA inclut la capacité 3DES par défaut pour l'accès de gestion uniquement, de sorte que vous pouvez vous connecter au gestionnaire de logiciels intelligents et utiliser ASDM immédiatement. Vous pouvez également utiliser SSH et SCP si vous configurez ultérieurement l'accès SSH sur l'ASA. D'autres fonctions qui nécessitent un cryptage renforcé (comme le VPN) doivent avoir le cryptage renforcé activé, ce qui exige que vous vous inscriviez d'abord au Smart Software Manager.



Remarque Si vous tentez de configurer des fonctions pouvant utiliser un cryptage renforcé avant de vous inscrire - même si vous ne configurez qu'un cryptage faible - votre connexion HTTPS sera interrompue sur cette interface, et vous ne pourrez pas vous reconnecter. Il y a une exception à cette règle si vous êtes connecté à une interface de gestion uniquement, telle que Management 1/1. SSH n'est pas affecté. Si vous perdez votre connexion HTTPS, vous pouvez vous connecter au port de console pour reconfigurer l'ASA, vous connecter à une interface de gestion uniquement, ou vous connecter à une interface non configurée pour une fonction de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour l'ASA à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation). Si l'ASA devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA continuera d'autoriser le trafic de transit. Même si vous réenregistrez l'ASA et que la conformité à l'exportation est désactivée, la licence reste activée. La licence est supprimée si vous restaurez l'ASA aux paramètres d'usine par défaut.

Si vous enregistrez initialement l'ASA sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'ASA pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

Cryptage renforcé : Firepower 2100 en mode plateforme

Le cryptage renforcé (3DES/AES) est disponible pour les connexions de gestion avant de vous connecter au Smart Software Manager ou au serveur Smart Software Manager sur site afin que vous puissiez lancer ASDM. Notez que l'accès ASDM est disponible sur les interfaces de gestion uniquement avec le chiffrement par défaut. Le trafic de transit qui nécessite un cryptage renforcé (comme VPN) n'est pas autorisé jusqu'à ce que vous vous connectiez et obteniez la licence de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour l'ASA à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation). Si l'ASA devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA continuera d'autoriser le trafic de transit. Même si vous réenregistrez l'ASA et que la conformité à l'exportation est désactivée, la licence reste activée. La licence est supprimée si vous restaurez l'ASA aux paramètres d'usine par défaut.

Si vous enregistrez initialement l'ASA sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'ASA pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

Cryptage renforcé : Châssis Firepower 4100/9300

Lorsque l'ASA est déployé en tant que périphérique logique, vous pouvez lancer ASDM immédiatement. Le trafic de transit qui nécessite un cryptage renforcé (comme VPN) n'est pas autorisé jusqu'à ce que vous vous connectiez et obteniez la licence de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour le châssis à partir de votre compte d'octroi de licences logicielles Smart, cochez la case **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce jeton) pour que la licence de cryptage renforcé (3DES/AES) soit appliquée (votre compte doit être qualifié pour son utilisation).

Si l'ASA devient non conforme par la suite, tant que le jeton de conformité à l'exportation a été appliqué avec succès, l'ASA continuera d'autoriser le trafic de transit. La licence est supprimée si vous réenregistrez le châssis et que la conformité à l'exportation est désactivée, ou si vous restaurez les paramètres d'usine par défaut du châssis.

Si vous enregistrez initialement le châssis sans cryptage renforcé, puis ajoutez ultérieurement le cryptage renforcé, vous devez recharger l'application ASA pour que la nouvelle licence prenne effet.

Pour les licences de réservation de licences permanentes, la licence de cryptage renforcé (3DES/AES) est activée si votre compte est admissible à son utilisation.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

DES : tous les modèles

Si le cryptage renforcé est activé, vous ne pouvez pas utiliser DES.

Licence d'opérateur

La licence d'opérateur permet d'utiliser les fonctionnalités d'inspection suivantes :

- Diameter : Diameter est un protocole d'authentification, d'autorisation et de comptabilité (AAA) utilisé dans les réseaux de télécommunications fixes et mobiles de nouvelle génération tels que SPE (Evolved Packet System) pour LTE (Long Term Évolution) et IMS (IP Multimédia Subsystem). Il remplace RADIUS et TACACS dans ces réseaux.
- GTP/GPRS : le protocole de tunnellisation GPRS est utilisé dans les réseaux SMS, UMTS et LTE pour le trafic du service radio général par paquets (GPRS). GTP fournit un protocole de gestion et de contrôle de tunnel pour fournir un accès réseau GPRS à une station mobile par la création, la modification et la suppression de tunnels. GTP utilise également un mécanisme de tunnellisation pour acheminer les paquets de données des utilisateurs.
- M3UA : MTP3 User Adaptation (M3UA) est un protocole client/serveur qui fournit une passerelle vers le réseau SS7 pour les applications IP qui communiquent avec la couche MTP3 (Message Transfer Part 3) de SS7. M3UA permet d'exécuter les composants SS7 (comme ISUP) sur un réseau IP. M3UA est défini dans la RFC 4666.
- SCTP : le protocole SCTP (Stream Control Transmission Protocol) est décrit dans la RFC 4960. Le protocole prend en charge le protocole de signalisation téléphonique SS7 sur IP et est également un protocole de transport pour plusieurs interfaces dans l'architecture de réseau mobile LTE 4G.

Nombre total de sessions de mandataire TLS

Chaque session de mandataire TLS pour l'inspection vocale chiffrée est prise en compte dans la limite de licences TLS.

D'autres applications qui utilisent des sessions de mandataire TLS ne sont pas prises en compte dans la limite du TLS, par exemple, le mandataire Mobility Advantage (qui ne nécessite pas de licence).

Certaines applications peuvent utiliser plusieurs sessions pour une connexion. Par exemple, si vous configurez un téléphone avec un Cisco Unified Communications Manager principal et de secours, il y a 2 connexions de mandataire TLS.

Vous définissez indépendamment la limite de mandataire TLS à l'aide de la commande **tls-proxy maximum-sessions** ou dans ASDM, en utilisant le volet **Configuration > Firewall (Pare-feu) > Unified Communications (Communications unifiées) > TLS Proxy (Mandataire TLS)**. Pour afficher les limites de votre modèle, saisissez la commande **tls-proxy maximum-sessions ?**. Lorsque vous appliquez une licence de mandataire TLS supérieure à la limite de mandataire TLS par défaut, l'ASA définit automatiquement la limite de mandataire TLS pour correspondre à la licence. La limite de mandataire TLS a priorité sur la limite de la licence; si vous définissez la limite de mandataire TLS pour qu'elle soit inférieure à la licence, vous ne pouvez pas utiliser toutes les sessions de votre licence.

Remarque Pour les licences dont la référence se termine par « K8 » (par exemple, les licences de moins de 250 utilisateurs), les sessions de mandataire TLS sont limitées à 1 000. Pour les licences dont la référence se termine par « K9 » (par exemple, les licences de 250 utilisateurs ou plus), la limite de mandataire TLS dépend de la configuration, jusqu'à la limite du modèle. K8 et K9 indiquent si la licence est restreinte pour l'exportation : la licence K8 n'est pas limitée tandis que la licence K9 est restreinte.

Si vous effacez la configuration (à l'aide de la commande **clear configure all**, par exemple), la limite de mandataire TLS est définie par défaut pour votre modèle; si cette valeur par défaut est inférieure à la limite de licence, vous verrez un message d'erreur pour utiliser la commande **tls-proxy maximum-sessions** afin d'augmenter à nouveau la limite (dans ASDM, utilisez le volet **TLS Proxy** (Mandataire TLS)). Si vous utilisez le basculement et saisissez la commande **write standby** ou dans ASDM, utilisez **File (Fichier) > Save Running Configuration to Standby Unit (Enregistrer la configuration d'exécution sur l'unité en veille)** sur l'unité principale pour forcer une synchronisation de la configuration; la commande **clear configure all** est générée automatiquement sur l'unité secondaire, vous pouvez donc voir le message d'avertissement sur l'unité secondaire. Étant donné que la synchronisation de la configuration restaure la limite de mandataire TLS définie sur l'unité principale, vous pouvez ignorer l'avertissement.

Vous pouvez également utiliser des sessions de chiffrement SRTP pour vos connexions :

- Pour les licences K8, les sessions SRTP sont limitées à 250.
- Pour les licences K9, il n'y a pas de limite.

Remarque Seuls les appels qui nécessitent un chiffrement ou un déchiffrement pour un support sont pris en compte dans la limite du SRTP; si la transmission est définie pour l'appel, même si les deux segments sont des SRTP, ils ne sont pas pris en compte dans la limite.

Nombre maximum de VLAN

Pour qu'une interface soit prise en compte dans la limite de VLAN, vous devez lui attribuer un VLAN. Par exemple :

```
interface gigabitethernet 0/0.100
vlan 100
```

Licence de filtre de trafic de réseau de zombies

Nécessite une licence de cryptage renforcé (3DES/AES) pour télécharger la base de données dynamique.

Licences de basculement ou de grappe ASA

Licences de basculement pour l'ASAv

L'unité en veille requiert le même modèle de licence que l'unité principale.

Licences de basculement pour Firepower 1010

Smart Software Manager standard et sur site

Les deux unités Firepower 1010 doivent être enregistrées auprès du serveur Smart Software Manager ou du Smart Software Manager sur site. Les deux unités nécessitent que vous activiez la licence Essentials et la licence Security Plus *avant* de pouvoir configurer le basculement.

En règle générale, vous n'avez pas également besoin d'activer la licence de fonction de cryptage renforcé (3DES/AES) dans l'ASA, car les deux unités devraient avoir obtenu le jeton de cryptage renforcé lorsque vous avez enregistré les unités. Lors de l'utilisation du jeton d'enregistrement, les deux unités doivent avoir le même niveau de chiffrement.

Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Dans ce cas, activez-la sur l'unité active après avoir activé le basculement. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. Seule l'unité active demande la licence au serveur. La licence est agrégée en une seule licence de basculement partagée par la paire de basculement, et cette licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement. Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce et que vous n'utilisez pas le jeton de cryptage renforcé, vous ne pourrez pas apporter de modifications de configuration aux fonctionnalités nécessitant la licence de fonctionnalité de cryptage renforcé (3DES/AES); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour Firepower 1100

Smart Software Manager standard et sur site

Seule l'unité active demande des licences auprès du serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement. Il n'y a pas de frais supplémentaires pour les unités secondaires.

Après avoir activé le basculement, pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. La licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement.

Remarque Chaque ASA doit avoir la même licence de chiffrement lors de la formation d'une paire de basculement. Lorsque vous enregistrez un ASA sur le serveur de licences Smart, la licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. En raison de cette exigence, vous avez deux choix de licence lorsque vous utilisez le jeton de cryptage renforcé avec le basculement:

- Avant d'activer le basculement, enregistrez les deux unités sur le serveur de licences smart. Dans ce cas, les deux unités auront un cryptage renforcé. Ensuite, après avoir activé le basculement, continuez de configurer les droits de licence sur l'unité active. Si vous activez le chiffrement pour le liaison de basculement, il utilisera AES/3DES (cryptage renforcé).
- Avant d'enregistrer l'unité active sur le serveur de licences smart, activez le basculement. Dans ce cas, les deux unités n'auront pas encore de cryptage renforcé. Configurez ensuite les droits de licence et enregistrez l'unité active sur le serveur de licences smart; les deux unités obtiendront un cryptage renforcé de la licence agrégée. Notez que si vous avez activé le chiffrement sur la liaison de basculement, il utilisera des DES (chiffrement faible), car la liaison de basculement a été établie avant que les unités n'acquièrent le cryptage renforcé. Vous devez recharger *les deux* unités pour utiliser AES/3DES sur la liaison. Si vous ne rechargez qu'une seule unité, cette unité tentera d'utiliser AES/ 3DES pendant que l'unité d'origine utilise DES, ce qui rendra active les deux unités (déconnexion cérébrale).

Chaque type de licence complémentaire est géré comme suit :

- Essentials : bien que seule l'unité active demande cette licence au serveur, l'unité en veille a la licence Essentials activée par défaut; elle n'a pas besoin de s'inscrire auprès du serveur pour l'utiliser.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 2 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 2 contextes; pour deux unités Firepower 1120, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 3 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 7 contextes. Cependant, comme la limite de plateformes pour une unité est de 5, la licence combinée autorise un maximum de 5 contextes uniquement. Dans ce cas, vous pourriez uniquement configurer la licence de contexte active pour 1 contexte.
  - Active/actif : la licence Essentials comprend 2 contextes; pour deux unités Firepower 1140, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 4 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 8 contextes. Une unité peut utiliser 5 contextes et l'autre unité peut utiliser 3 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 8. Comme la limite de plateformes pour une unité est de 10, la licence combinée autorise un maximum de 10 contextes; les 8 contextes sont dans la limite.
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne

unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales (c.-à-d. ajouter un contexte supplémentaire); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour Firepower 2100

Smart Software Manager standard et sur site

Seule l'unité active demande des licences auprès du serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement. Il n'y a pas de frais supplémentaires pour les unités secondaires.

Après avoir activé le basculement, pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. La licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement.



Remarque Chaque ASA doit avoir la même licence de chiffrement lors de la formation d'une paire de basculement. Lorsque vous enregistrez un ASA sur le serveur de licences Smart, la licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. En raison de cette exigence, vous avez deux choix de licence lorsque vous utilisez le jeton de cryptage renforcé avec le basculement:

- Avant d'activer le basculement, enregistrez les deux unités sur le serveur de licences smart. Dans ce cas, les deux unités auront un cryptage renforcé. Ensuite, après avoir activé le basculement, continuez de configurer les droits de licence sur l'unité active. Si vous activez le chiffrement pour le liaison de basculement, il utilisera AES/3DES (cryptage renforcé).
- Avant d'enregistrer l'unité active sur le serveur de licences smart, activez le basculement. Dans ce cas, les deux unités n'auront pas encore de cryptage renforcé. Configurez ensuite les droits de licence et enregistrez l'unité active sur le serveur de licences smart; les deux unités obtiendront un cryptage renforcé de la licence agrégée. Notez que si vous avez activé le chiffrement sur la liaison de basculement, il utilisera des DES (chiffrement faible), car la liaison de basculement a été établie avant que les unités n'acquièrent le cryptage renforcé. Vous devez recharger *les deux* unités pour utiliser AES/3DES sur la liaison. Si vous ne rechargez qu'une seule unité, cette unité tentera d'utiliser AES/ 3DES pendant que l'unité d'origine utilise DES, ce qui rendra active les deux unités (déconnexion cérébrale).

Chaque type de licence complémentaire est géré comme suit :

- Essentials : bien que seule l'unité active demande cette licence au serveur, l'unité en veille a la licence Essentials activée par défaut; elle n'a pas besoin de s'inscrire auprès du serveur pour l'utiliser.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 2 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 2 contextes; pour deux unités Firepower 2130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 30 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 34 contextes. Cependant, comme la limite de plateformes pour une unité est de 30, la licence combinée autorise un maximum de 30 contextes uniquement. Dans ce cas, vous pourriez uniquement configurer la licence de contexte active pour 25 contextes.
  - Active/actif : la licence Essentials comprend 2 contextes; pour deux unités Firepower 2130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 10 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 14 contextes. Une unité peut utiliser 9 contextes et l'autre unité peut utiliser 5 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 14. Comme la limite de plateformes pour une unité est de 30, la licence combinée autorise un maximum de 30 contextes; les 14 contextes sont dans la limite.
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales (c.-à-d. ajouter un contexte supplémentaire); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour Cisco Secure Firewall 3100

Smart Software Manager standard et sur site

Chaque unité requiert la licence Essentials (activée par défaut) et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer le basculement pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de basculement.

La fonctionnalité de basculement elle-même ne nécessite aucune licence. Il n'y a pas de coût supplémentaire pour la licence de contexte sur les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, la licence Essentials est toujours activée par défaut sur les deux unités. Après avoir activé le basculement, pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. La licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement.

Chaque type de licence complémentaire est géré comme suit :

- Essentials : chaque unité demande une licence Essentials au serveur.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 2 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 2 contextes; pour deux unités Secure Firewall 3130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 100 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 104 contextes. Cependant, comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes uniquement. Dans ce cas, vous pourriez uniquement configurer la licence de contexte active pour 95 contextes.
  - Active/active : la licence Essentials comprend 2 contextes; pour deux unités Secure Firewall 3130, ces licences ajoutent jusqu'à 4 contextes. Vous configurez une licence de 10 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 14 contextes. Une unité peut utiliser 9 contextes et l'autre unité peut utiliser 5 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 14. Comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes; les 14 contextes sont dans la limite.
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales (c.-à-d. ajouter un contexte supplémentaire); l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état

mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de basculement pour l'Firepower 4100/9300

Smart Software Manager standard et sur site

Les deux Firepower 4100/9300 doivent être enregistrés auprès du Smart Software Manager ou du Smart Software Manager sur site avant de configurer le basculement. Il n'y a pas de frais supplémentaires pour les unités secondaires.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Lors de l'utilisation du jeton, chaque châssis doit avoir la même licence de chiffrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Après avoir activé le basculement, pour la configuration de la licence ASA pour le basculement actif/veille, vous pouvez uniquement configurer la licence Smart sur l'unité active. Pour le basculement actif/actif, vous pouvez uniquement configurer la licence Smart sur l'unité avec le groupe de basculement 1 comme actif. La configuration est répliquée sur l'unité en veille, mais cette dernière n'utilise pas la configuration; elle reste dans un état mis en mémoire cache. Seule l'unité active demande les licences auprès du serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement, et cette licence agrégée est également mise en mémoire cache sur l'unité en veille pour être utilisée si elle devient l'unité active ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : bien que seule l'unité active demande cette licence au serveur, l'unité en veille a la licence Essentials activée par défaut; elle n'a pas besoin de s'inscrire auprès du serveur pour l'utiliser.
- Contexte : seule l'unité active demande cette licence. Cependant, la licence Essentials comprend 10 contextes par défaut et est présente sur les deux unités. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité active, sont combinées jusqu'à la limite de plateformes. Par exemple :
  - Active/en veille : la licence Essentials comprend 10 contextes; pour 2 unités, ces licences ajoutent jusqu'à 20 contextes. Vous configurez une licence de 250 contextes sur l'unité active dans une paire active/en veille. Par conséquent, la licence de basculement agrégée comprend 270 contextes. Cependant, comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes uniquement. Dans ce cas, vous devez configurer uniquement la licence de contexte active pour 230 contextes.
  - Active/active : la licence Essentials comprend 10 contextes; pour 2 unités, ces licences ajoutent jusqu'à 20 contextes. Vous configurez une licence de 10 contextes sur l'unité principale dans une paire active/active. Par conséquent, la licence de basculement agrégée comprend 30 contextes. Une unité peut utiliser 17 contextes et l'autre unité peut utiliser 13 contextes, par exemple; mais en cas de défaillance, une unité utilisera les 30. Comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes; les 30 contextes sont dans la limite.
- Opérateur : seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

- Cryptage renforcé (3DES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Après un basculement, la nouvelle unité active continue d'utiliser la licence agrégée. Elle utilise la configuration de la licence mise en mémoire cache pour demander à nouveau l'autorisation au serveur. Lorsque l'ancienne unité active rejoint la paire en tant qu'unité de veille, elle libère le droit de licence. Avant que l'unité en veille ne libère le droit, la licence de la nouvelle unité active peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La paire de basculement peut utiliser la licence agrégée pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Si vous annulez la paire de basculement, l'unité active libère les droits et les deux unités conservent la configuration de licence en état mis en mémoire cache. Pour réactiver la licence, vous devez effacer la configuration sur chaque unité et la reconfigurer.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer le basculement.

Licences de grappe ASA pour Cisco Secure Firewall 3100

Smart Software Manager standard et sur site

Chaque unité requiert la licence Essentials (activée par défaut) et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer la mise en grappe pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de commande de grappe.

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Il n'y a pas de coût supplémentaire pour la licence de contexte sur les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, la licence Essentials est toujours activée par défaut sur toutes les unités. Vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : chaque unité demande une licence Essentials au serveur.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 2 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :
  - Vous avez 6 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 6 unités, ces licences ajoutent jusqu'à 12 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée

comprend 32 contextes. Comme la limite de plateformes pour un châssis est de 100, la licence combinée autorise un maximum de 100 contextes; les 32 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 32 contextes sur l'unité de contrôle; chaque unité de données aura également 32 contextes par la réplication de la configuration.

- Vous avez 3 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 3 unités, ces licences ajoutent jusqu'à 6 contextes. Vous configurez une licence de 100 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 106 contextes. Comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes; les 106 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 100 contextes sur l'unité de contrôle; chaque unité de données aura également 100 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 94 contextes.

- Cryptage renforcé (3DES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité de contrôle demande cette licence et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Licences de grappe ASA pour l'ASAv

Smart Software Manager standard et sur site

Chaque unité nécessite la même licence de débit et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer la mise en grappe pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de commande de grappe.

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent

pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : seule l'unité de contrôle demande la licence Essentials au serveur et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.
- Débit : chaque unité demande sa propre licence de débit auprès du serveur.
- Cryptage renforcé (3DES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité de contrôle demande cette licence et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque unité et activer les licences *avant* de configurer la mise en grappe.

Licences de grappe ASA pour l'Firepower 4100/9300

Smart Software Manager standard et sur site

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Pour utiliser le cryptage renforcé et d'autres licences facultatives, chaque Châssis Firepower 4100/9300 doit être enregistré auprès de l'autorité de licence ou du serveur Smart Software Manager standard et sur site. Il n'y a pas de frais supplémentaires pour les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Lors de l'utilisation du jeton, chaque châssis doit avoir la même licence de chiffrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : seule l'unité de contrôle demande la licence Essentials au serveur et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 10 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :
  - Vous avez 6 modules Firepower 9300 dans la grappe. La licence Essentials comprend 10 contextes; pour 6 unités, ces licences ajoutent jusqu'à 60 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 80 contextes. Comme la limite de plateformes pour un module est de 250, la licence combinée autorise un maximum de 250 contextes; les 80 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 80 contextes sur l'unité de contrôle; chaque unité de données aura également 80 contextes par la réplication de la configuration.

- Vous avez 3 unités Firepower 4112 dans la grappe. La licence Essentials comprend 10 contextes; pour 3 unités, ces licences ajoutent jusqu'à 30 contextes. Vous configurez une licence de 250 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 280 contextes. Comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes; les 280 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 250 contextes sur l'unité de contrôle; chaque unité de données aura également 250 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 220 contextes.

- Opérateur : requis pour le VPN S2S distribué. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.
- Cryptage renforcé (3DES) : pour un déploiement Cisco Smart Software Manager sur site antérieur à la version 2.3.0, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement d'autorisation toutes les 12 heures jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Conditions préalables à la gestion de licences logicielles Smart

Conditions préalables de Smart Software Manager standard et sur site

Firepower 4100/9300

Configurez l'infrastructure de licence logicielle Smart sur le Châssis Firepower 4100/9300 avant de configurer les droits de licence ASA.

Tous les autres modèles

- Assurez-vous de l'accès Internet, de l'accès au mandataire HTTP ou de l'accès au serveur Smart Software Manager sur site à partir du périphérique.

- Configurez un serveur DNS pour que le périphérique puisse résoudre le nom du Smart Software Manager.
- Réglez l'horloge du périphérique. Sur le Firepower 2100 en mode plateforme, vous réglez l'horloge dans FXOS.
- Créez un compte sur le Cisco Smart Software Manager :

  https://software.cisco.com/#module/SmartLicensing

  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte pour votre organisation.

Conditions préalables à la réservation de licence permanente

- Créez un compte principal sur le Cisco Smart Software Manager :

  https://software.cisco.com/#module/SmartLicensing

  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation. Même si l'ASA a besoin d'une connectivité Internet au serveur de licences Smart pour la réservation de licence permanente, Smart Software Manager est utilisé pour gérer vos licences permanentes.
- Obtenez une assistance pour la réservation de licence permanente de l'équipe chargée des licences. Vous devez fournir une justification pour utiliser la réservation de licence permanente. Si votre compte n'est pas approuvé, vous ne pouvez pas acheter et appliquer de licences permanentes.
- Achetez des licences permanentes spéciales (voir PID de licence par modèle, à la page 161). Si vous n'avez pas la bonne licence dans votre compte, lorsque vous essayez de réserver une licence sur l'ASA, vous verrez un message d'erreur ressemblant à : « Les licences ne peuvent pas être réservées, car le compte virtuel ne contient pas un surplus suffisant des licences permanentes suivantes : 1 – Firepower 4100 ASA PERM UNIV (perpétuelle) ».
- La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat d'une licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).
- ASA virtuel : la réservation de licence permanente n'est pas prise en charge pour l'hyperviseur Azure.

Gestion des licences logicielles Smart

- Seules les licences logicielles Smart sont prises en charge. Pour les anciens logiciels sur l'ASA virtuel, si vous mettez à niveau un ASA virtuel sous licence PAK existant, la clé d'activation précédemment installée sera ignorée, mais conservée sur l'appareil. Si vous rétrogradez l'ASA virtuel, la clé d'activation sera rétablie.
- Pour la réservation de licence permanente, vous devez retourner la licence avant de désactiver l'appareil. Si vous ne retournez pas officiellement la licence, la licence reste dans un état usagé et ne peut pas être réutilisée pour un nouvel appareil.

- Étant donné que la passerelle de transmission Cisco utilise un certificat avec un code de pays non conforme, vous ne pouvez pas utiliser HTTPS lorsque vous utilisez l'ASA en conjonction avec ce produit. Vous devez utiliser HTTP avec la passerelle de transmission Cisco.

Paramètres par défaut des licences logicielles Smart

Profil Smart Call Home

La configuration par défaut pour tous les modèles, à l'exception des modèles Firepower 4100/9300 (qui active la communication de la licence logicielle Smart au niveau du châssis), comprend un profil Smart Call Home appelé « Licence » qui spécifie l'URL de Smart Software Manager.

```
call-home
  profile License
   destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

ASA virtuel

- Lorsque vous déployez l'ASA virtuel, vous définissez le niveau de fonctionnalité et le niveau de débit. Seul le niveau Essentials est disponible pour le moment. Pour la réservation de licence permanente, vous n'avez pas besoin de définir ces paramètres. Lorsque vous activez la réservation de licence permanente, ces commandes sont supprimées de la configuration.



Remarque La licence Essentials était connue sous le nom de licence Standard, et l'interface de ligne de commande utilise toujours la terminologie « Standard ».

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

ASA virtuel : configurer les licences logicielles Smart

Cette section décrit comment configurer les licences logicielles Smart pour ASA virtuel.

ASA virtuel : configurer les licences logicielles Smart standard

Lorsque vous déployez l'ASA virtuel, vous pouvez préconfigurer le périphérique et inclure un jeton d'enregistrement afin qu'il s'enregistre auprès du Smart Software Manager et active les licences logicielles Smart. Si vous devez modifier votre serveur mandataire HTTP, vos droits de licence ou enregistrer l'ASA virtuel (par exemple, si vous n'avez pas inclus le jeton d'identification dans la configuration Day0), effectuez cette tâche.

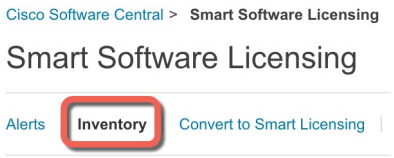
Remarque Vous avez peut-être préconfiguré le mandataire HTTP et les droits de licence lorsque vous avez déployé votre ASA virtuel. Vous avez peut-être également inclus le jeton d'enregistrement dans votre configuration Day0 lorsque vous avez déployé l'ASA virtuel; si tel est le cas, vous n'avez pas besoin de vous réinscrire en utilisant cette procédure.

Procédure

Étape 1 (Cisco Smart Software Manager), demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

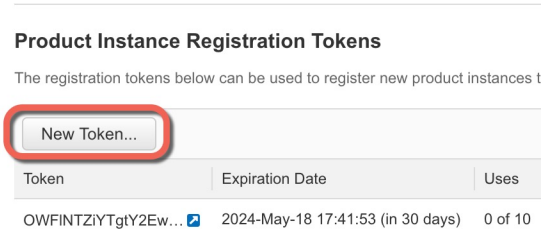
a) Cliquez sur **Inventory** (Inventaire).

Illustration 8 : Inventaire



b) Dans l'onglet **General** (Général), cliquez sur **New Token** (Nouveau jeton).

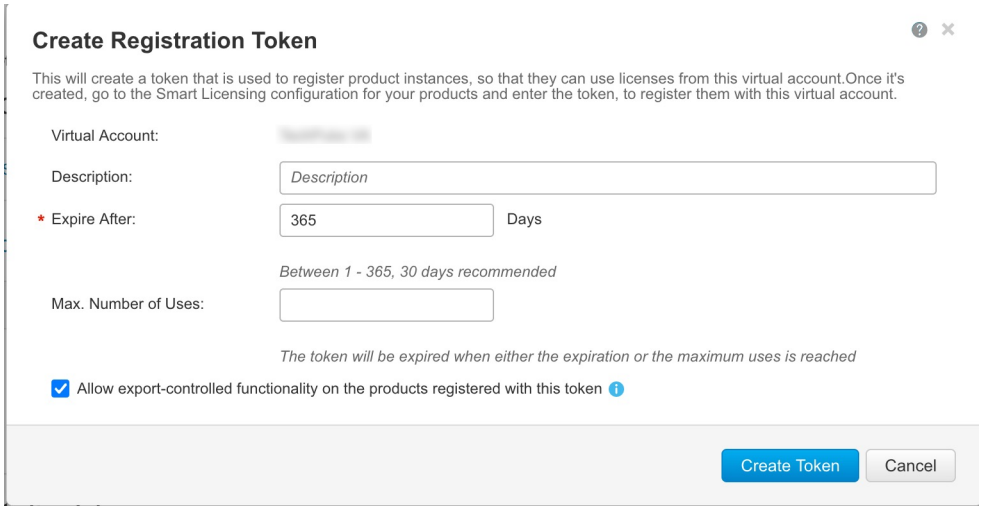
Illustration 9 : Nouveau jeton



c) Dans la boîte de dialogue **Create Registration Token** (Créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (Créer un jeton) :

- **Description**
- **Expire After** (Expiration après) : Cisco recommande 30 jours.
- **Nombre max. d'utilisations**
- **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton) : active l'indicateur de conformité à l'exportation.

Illustration 10 : Créer un jeton d'enregistrement



Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (Jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Gardez ce jeton prêt pour plus tard dans la procédure lorsque vous devez enregistrer ASA.

Illustration 11 : Afficher le jeton

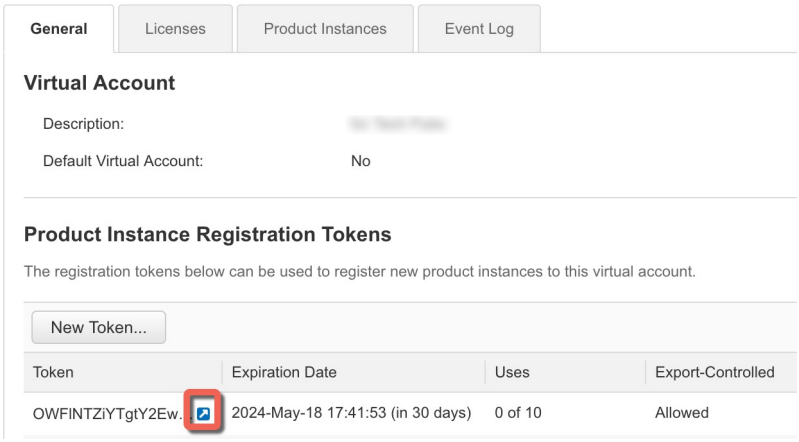
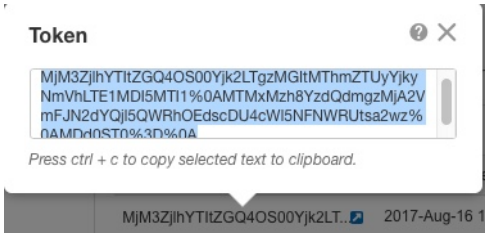


Illustration 12 : Copier le jeton



Étape 2 (Facultatif) Sur l'ASA virtuel, spécifiez l'URL du mandataire HTTP pour Call Home :

call-home

http-proxy *ip_address* **port** *port*

Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configuer l'adresse du mandataire pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Transport et Smart Call Home en général.

Remarque
Le mandataire HTTP avec l'authentification n'est pas pris en charge.

Exemple :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

Étape 3 Configurez les droits de licence :

a) Entrez en mode de configuration de la licence Smart :

licence smart

Exemple :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) Définissez le niveau de fonctionnalité :

niveau de fonctionnalité standard

Seul le niveau Standard (Essentials) est disponible, cependant, vous devez l'activer dans la configuration. La licence Essentials était auparavant appelée licence Standard, et « Standard » est toujours utilisé dans l'interface de ligne de commande.

c) Définissez le niveau de débit pour déterminer la licence demandée à Smart Software Manager :

throughput level {**100M** | **1G** | **2G** | **10G** | **20G**}

Consultez la relation débit/licence suivante :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

Exemple :

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) (Facultatif) Activez le cryptage renforcé. **Ne saisissez pas** cette commande si vous recevez le jeton de cryptage renforcé.

feature strong-encryption

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Remarque
Si vous saisissez cette commande, votre appareil utilisera la licence de cryptage renforcé, qu'elle soit nécessaire ou non. Donc, à moins que vous n'ayez cette licence dans votre compte, votre compte ne sera pas conforme. Étant donné que cette licence n'est pas nécessaire lors de l'utilisation du jeton de cryptage renforcé, vous pouvez accidentellement rendre votre compte non conforme sans aucun avantage.

Exemple :

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

e) Quittez le mode de licence Smart pour appliquer vos modifications :

exit

Vos modifications ne prennent effet que lorsque vous quittez le mode de configuration de la licence Smart, soit en sortant explicitement du mode (**quitter** ou **terminer**) ou en saisissant une commande qui vous amène à un autre mode.

Exemple :

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Étape 4 Enregistrez le ASA virtuel auprès du Smart Software Manager

license smart register idtoken *id_token* [**force**]

L'ASA virtuel tente de s'enregistrer auprès de Smart Software Manager et demande l'autorisation pour les droits de licence configurés.

Lorsque vous enregistrez l'ASA virtuel, Smart Software Manager émet un certificat d'ID pour la communication entre l'ASA virtuel et Smart Software Manager. Il affecte également l'ASA virtuel au compte virtuel approprié. Normalement, cette procédure est une instance unique. Cependant, vous devrez peut-être réenregistrer ultérieurement l'ASA virtuel si le certificat d'ID expire en raison d'un problème de communication, par exemple.

Utilisez le mot clé **force** pour enregistrer l'ASA virtuel qui est déjà enregistré, mais qui pourrait ne pas être synchronisé avec Cisco Smart Software Manager. Par exemple, utilisez **force** si l'ASA virtuel a été accidentellement retiré de Cisco Smart Software Manager.

Exemple :

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

Étape 5 Vérifiez l'état de la licence.

show license status ou **show running-config license**

Si la communication avec Smart Software Manager échoue, vérifiez que vous avez configuré un serveur DNS et le bon routage pour atteindre le serveur.

Exemple :

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERING - REGISTRATION IN PROGRESS
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Aug 31 2023 19:38:45 UTC
    Failure reason: Communication message send error
  Next Registration Attempt: Aug 31 2023 19:56:56 UTC

License Authorization:
  Status: EVAL EXPIRED on Feb 25 2023 16:39:25 UTC

Export Authorization Key:
  Features Authorized:
    <none>

Miscellaneus:
  Custom Id: <empty>
```

ASA virtuel : configurer les licences Smart Software Manager sur site

Cette procédure s'applique pour l'ASA virtuel à l'aide de Smart Software Manager sur site.

Avant de commencer

- Téléchargez le fichier OVA Smart Software Manager sur site à partir de Cisco.com, installez-le et configurez-le sur un serveur VMwareESXi. Pour en savoir plus, consultez la *fiche technique de Cisco Smart Software Manager sur site*.
- Téléchargez le groupe de confiance CA de chiffrement avant de placer l'appareil dans un réseau isolé. Ce groupe de confiance est normalement téléchargé automatiquement, mais peut être obsolète dans un réseau isolé :

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

Procédure

Étape 1 Demandez un jeton d'enregistrement sur Smart Software Manager sur site.

Étape 2 (Facultatif) Sur l'ASA virtuel, spécifiez l'URL du mandataire HTTP pour Call Home :

call-home

http-proxy *ip_address* **port** *port*

Remarque
Le mandataire HTTP avec l'authentification n'est pas pris en charge.

Exemple :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

Étape 3 Changez l'URL du serveur de licence pour accéder à Smart Software Manager sur site.

call-home

profile License

destination address http https://*on-prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

Exemple :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile) destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

Étape 4 Configurez les droits de licence.

a) Entrez en mode de configuration de la licence Smart :

licence smart

Exemple :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) Définissez le niveau de fonctionnalité :

niveau de fonctionnalité standard

Seul le niveau Standard (Essentials) est disponible, cependant, vous devez l'activer dans la configuration. La licence Essentials était auparavant appelée licence Standard, et **standard** est toujours utilisé dans l'interface de ligne de commande.

c) Définissez le niveau de débit pour déterminer la licence demandée à Smart Software Manager :

throughput level {**100M** | **1G** | **2G** | **10G** | **20G**}

Consultez la relation débit/licence suivante :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

Exemple :

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) (Facultatif) Activez le cryptage renforcé. **Ne saisissez pas** cette commande si vous recevez le jeton de cryptage renforcé.

feature strong-encryption

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Remarque
Si vous saisissez cette commande, votre appareil utilisera la licence de cryptage renforcé, qu'elle soit nécessaire ou non. Donc, à moins que vous n'ayez cette licence dans votre compte, votre compte ne sera pas conforme. Étant donné que cette licence n'est pas nécessaire lors de l'utilisation du jeton de cryptage renforcé, vous pouvez accidentellement rendre votre compte non conforme sans aucun avantage.

Exemple :

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

e) Quittez le mode de licence Smart pour appliquer vos modifications :

exit

Vos modifications ne prennent effet que lorsque vous quittez le mode de configuration de la licence Smart, soit en sortant explicitement du mode (**quitter** ou **terminer**) ou en saisissant une commande qui vous amène à un autre mode.

Exemple :

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Étape 5 Enregistrez l'ASA à l'aide du jeton que vous avez demandé à l'étape 1 :

license smart register idtoken *id_token*

L'ASA s'enregistre auprès de Smart Software Manager sur site et demande l'autorisation pour les droits de licence configurés. Smart Software Manager sur site applique également la licence de cryptage renforcé (3DES/AES) si votre compte le permet.

Lorsque vous enregistrez l'ASA virtuel, Smart Software Manager sur site émet un certificat d'ID pour la communication entre l'ASA virtuel et Smart Software Manager. Il affecte également l'ASA virtuel au compte virtuel approprié. Normalement, cette procédure est une instance unique. Cependant, vous devrez peut-être réenregistrer ultérieurement l'ASA virtuel si le certificat d'ID expire en raison d'un problème de communication, par exemple.

Exemple :

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

Étape 6 Vérifiez l'état de la licence.

show license status

Si la communication avec Smart Software Manager échoue, vérifiez que vous avez configuré un serveur DNS et le bon routage pour atteindre le serveur.

Exemple :

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERING - REGISTRATION IN PROGRESS
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Aug 31 2023 19:38:45 UTC
    Failure reason: Communication message send error
  Next Registration Attempt: Aug 31 2023 19:56:56 UTC

License Authorization:
  Status: EVAL EXPIRED on Feb 25 2023 16:39:25 UTC

Export Authorization Key:
  Features Authorized:
    <none>

Miscellaneus:
  Custom Id: <empty>
```

ASA virtuel: configurer les licences logicielles Smart Utility (MSLA)

La licence utilitaire pour un contrat de licence de services gérés (MSLA) vous permet de payer la durée d'utilisation d'une licence plutôt que de payer des frais ponctuels pour un abonnement à une licence ou une licence permanente. En mode de licence utilitaire, l'ASA virtuel suit l'utilisation des licences en unités de temps (intervalles de 15 minutes). L'ASA virtuel envoie des rapports d'utilisation des licences (aussi appelés rapports sur la mesure de l'utilisation des ressources) à Smart Software Manager toutes les quatre heures. Les rapports d'utilisation sont ensuite acheminés à un serveur de facturation. Avec les licences utilitaires, Smart Call Home n'est pas utilisé comme transport pour les messages de licence. Au lieu de cela, les messages sont envoyés directement via HTTP/HTTPS à l'aide de *Smart Transport*.

Avant de commencer

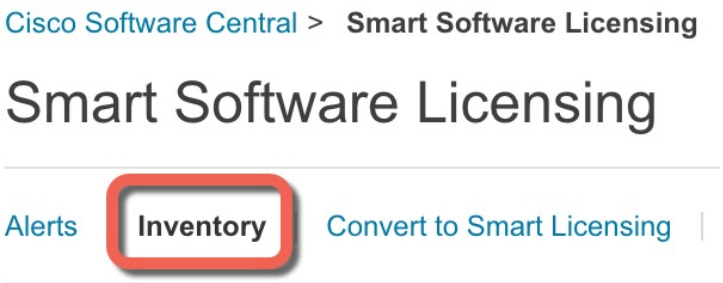
Si vous utilisez Smart Software Manager sur site, téléchargez le fichier OVA Smart Software Manager sur site à partir de Cisco.com, installez et configurez-le sur un serveur VMware ESXi. Pour en savoir plus, consultez la *fiche technique de Cisco Smart Software Manager sur site*.

Procédure

Étape 1 Dans Smart Software Manager (Cisco Smart Software Manager), demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

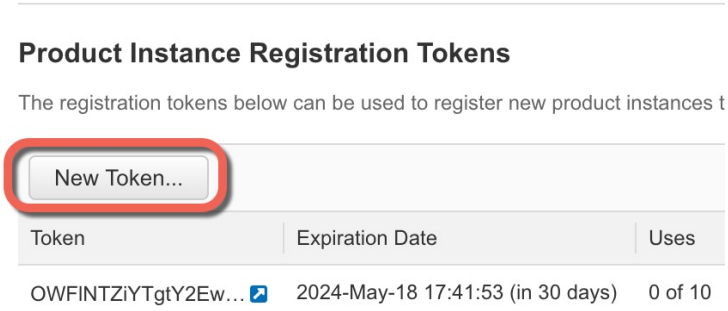
a) Cliquez sur **Inventory** (Inventaire).

Illustration 13 : Inventaire



b) Dans l'onglet **General** (Général), cliquez sur **New Token** (Nouveau jeton).

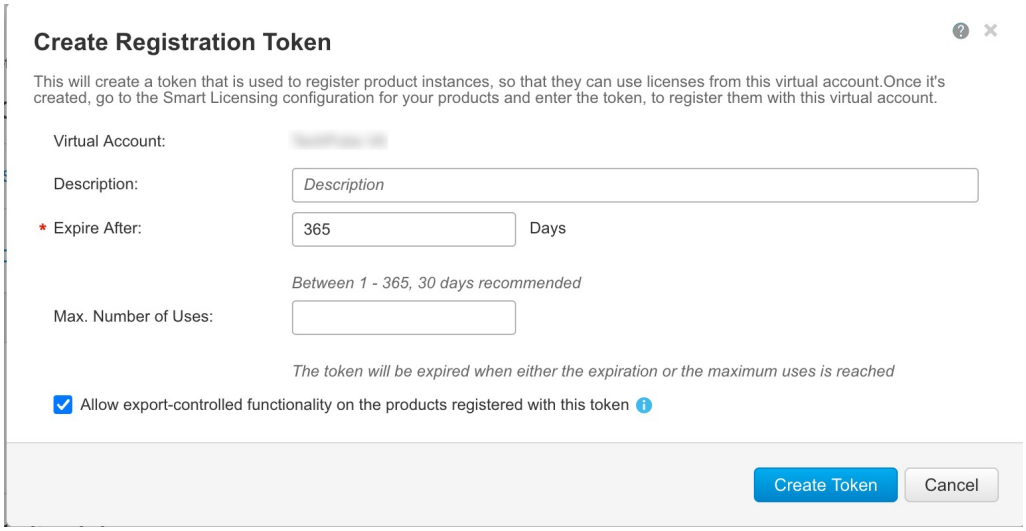
Illustration 14 : Nouveau jeton



c) Dans la boîte de dialogue **Create Registration Token** (Créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (Créer un jeton) :

- **Description**
- **Expire After** (Expiration après) : Cisco recommande 30 jours.
- **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton) : active l'indicateur de conformité à l'exportation.

Illustration 15 : Créer un jeton d'enregistrement



Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (Jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Gardez ce jeton prêt pour plus tard dans la procédure lorsque vous devez enregistrer ASA.

Illustration 16 : Afficher le jeton

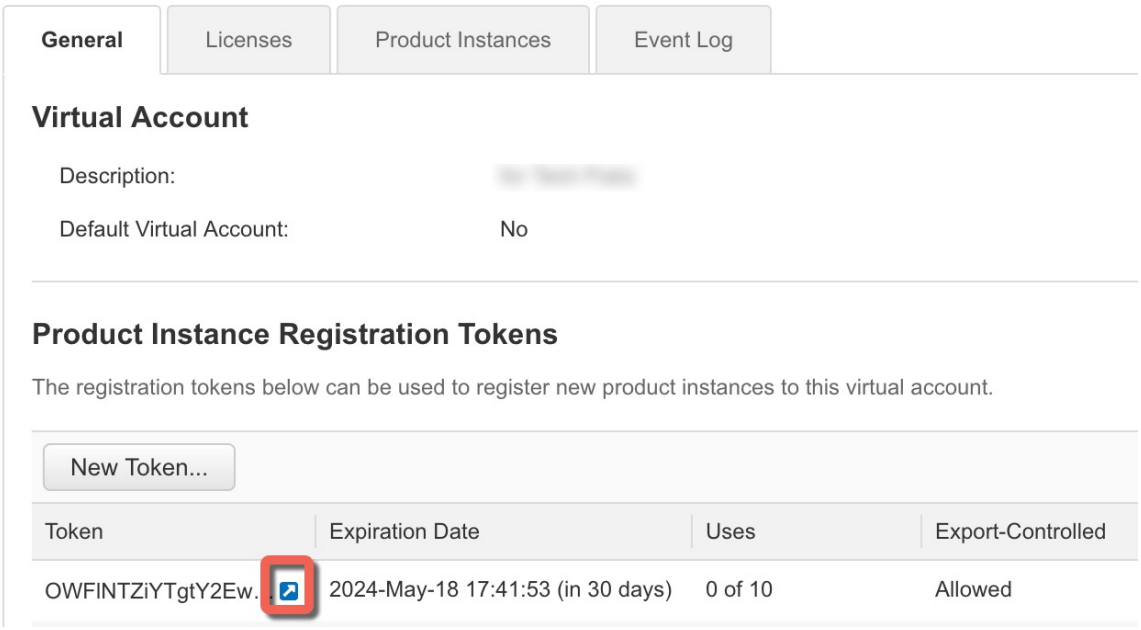
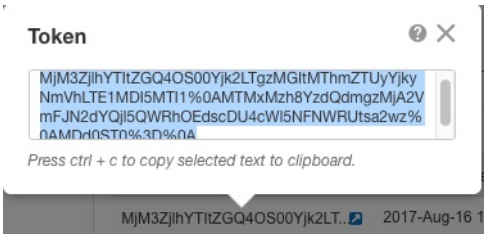


Illustration 17 : Copier le jeton



Étape 2 Sur l'ASA virtuel, configurez les paramètres de licence Smart.

a) Entrez en mode de configuration de la licence Smart.

license smart

Exemple :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) Activez Smart Transport.

transport type smart

Les licences utilitaires nécessitent Smart Transport au lieu de Smart Call Home.

Exemple :

```
ciscoasa(config-smart-lic)# transport type smart
```

c) (Facultatif) Spécifiez l'URL de Smart Software Manager standard ou sur site. Vous pouvez également spécifier une autre destination pour les rapports d'utilisation des licences.

transport url {*transport_url* | **utility** *utility_url* | **default** }

Si vous ne définissez pas d'URL, la valeur **default** est utilisée à la fois pour les rapports Smart Transport et les rapports d'utilisation des licences, à savoir, **https://smartreceiver.cisco.com/licservice/license**.

Exemple :

```
ciscoasa(config-smart-lic)# transport url http://server99.cisco.com/SmartTransport
ciscoasa(config-smart-lic)# transport url utility
http://server-utility.cisco.com/SmartTransport
```

d) (Facultatif) Si votre réseau utilise un mandataire HTTP pour accéder à Internet, configurez l'adresse du mandataire.

transport proxy *proxy-url* **port** *proxy-port-number*

Remarque
Le mandataire HTTP avec l'authentification n'est pas pris en charge.

Exemple :

```
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 443
```

e) Supprimez le nom d'hôte ou le numéro de version Smart Agent du périphérique de licence dans les messages de licence.

privacy {**all** | **hostname** | **version**}

Exemple :

```
ciscoasa(config-smart-lic)# privacy all
```

f) Définissez le niveau de fonctionnalité :

niveau de fonctionnalité standard

Seul le niveau Standard (Essentials) est disponible, cependant, vous devez l'activer dans la configuration. La licence Essentials était auparavant appelée licence Standard, et **standard** est toujours utilisé dans l'interface de ligne de commande.

g) Définissez le niveau de débit pour déterminer la licence demandée à Smart Software Manager :

throughput level {**100M** | **1G** | **2G** | **10G** | **20G**}

Consultez la relation débit/licence suivante :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

Exemple :

```
ciscoasa(config-smart-lic)# throughput level 2G
```

h) (Facultatif) Activez le cryptage renforcé.

feature strong-encryption

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Exemple :

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

i) Quittez le mode de licence Smart pour appliquer vos modifications :

exit

Vos modifications ne prennent effet que lorsque vous quittez le mode de configuration de la licence Smart, soit en sortant explicitement du mode (**quitter** ou **terminer**) ou en saisissant une commande qui vous amène à un autre mode.

Exemple :

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Étape 3 Configurez les licences utilitaires.

a) Entrez en mode de configuration utilitaire.

utility

Exemple :

```
ciscoasa(config-smart-lic)# utility
ciscoasa(config-smart-lic-util)#
```

b) Créez un identifiant client unique. Cet identifiant est inclus dans les messages du rapport d'utilisation des licences utilitaires.

custom-id *custom-identifier*

Exemple :

```
ciscoasa(config-smart-lic-util)# custom-id MyCustomID
```

c) Créez un profil de client unique. Ces renseignements sont inclus dans les rapports d'utilisation des licences utilitaires.

customer-info {**city** | **country** | **id** | **name** | **postalcode** | **state** |**street**} *value*

Exemple :

```
ciscoasa(config-smart-lic-util)# customer-info city MyCity
ciscoasa(config-smart-lic-util)# customer-info country MyCountry
ciscoasa(config-smart-lic-util)# customer-info id MyID
ciscoasa(config-smart-lic-util)# customer-info name MyName
ciscoasa(config-smart-lic-util)# customer-info postalcode MyPostalCode
ciscoasa(config-smart-lic-util)# customer-info state MyState
ciscoasa(config-smart-lic-util)# customer-info street MyStreet
```

d) Activez les licences utilitaires.

mode standard

Exemple :

```
ciscoasa(config-smart-lic-util)# mode standard
```

Étape 4 Enregistrez l'ASA à l'aide du jeton que vous avez demandé à l'étape 1 :

license smart register idtoken *id_token*

Exemple :

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

Étape 5 Vérifiez l'état de la licence.

show license status

Si la communication avec Smart Software Manager échoue, vérifiez que vous avez configuré un serveur DNS et le bon routage pour atteindre le serveur.

Exemple :

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: ENABLED
  Utility report:
    Last success: May 14 2018 21:37:25 UTC
    Last attempt: SUCCEEDED on May 14 2018 21:37:24 UTC
    Next attempt: May 15 2018 01:37:24 UTC

  Customer Information:
    Id: MyID
    Name: MyName
    Street: MyStreet
    City: MyCity
    State: MyState
    Country: MyCountry
    Postal Code: MyPostalCode
```

```
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Smart
  Registration URL: http://server99.cisco.com/SmartTransport
  Utility URL: http://server-utility.cisco.com/SmartTransport

Registration:
  Status: REGISTERED
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on May 14 2018 21:37:20 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Sep 13 2018 13:34:40 UTC
  Registration Expires: May 14 2019 21:29:20 UTC

License Authorization:
  Status: AUTHORIZED on May 14 2018 21:37:22 UTC
  Last Communication Attempt: NOT STARTED
    Failure reason: Device in Thirdparty Utility Mode
  Next Communication Attempt: None
  Communication Deadline: Aug 12 2018 21:37:24 UTC
```

ASA virtuel: configurer la réservation de licence permanente

Vous pouvez attribuer une licence permanente à l'ASA virtuel. Cette section décrit également comment restituer une licence si vous retirez l'ASA virtuel ou si vous modifiez les niveaux de modèle et que vous avez besoin d'une nouvelle licence.

Procédure

Étape 1 Installer la licence permanente ASA virtuel, à la page 128

Étape 2 (Facultatif) Retourner la licence permanente ASA virtuel, à la page 131

Installer la licence permanente ASA virtuel

Pour un ASA virtuel qui n'a pas d'accès Internet, vous pouvez demander une licence permanente auprès de Smart Software Manager. Pour en savoir plus sur la réservation de licence permanente ASA virtuel, consultez Réservation de licence permanente pour l'ASA virtuel, à la page 91.

Remarque

- Pour la réservation de licence permanente, vous devez retourner la licence avant de désactiver l'ASA virtuel. Si vous ne retournez pas officiellement la licence, la licence reste dans un état usagé et ne peut pas être réutilisée pour un nouvel ASA virtuel. Consultez (Facultatif) Retourner la licence permanente ASA virtuel, à la page 131.
- Si vous effacez votre configuration après avoir installé la licence permanente, par exemple, en utilisant la commande **write erase**, vous n'avez qu'à réactiver la réservation de licence permanente à l'aide de la commande **license smart reservation** sans arguments, vous n'avez pas besoin de terminer le reste de cette procédure.

Avant de commencer

- Achetez des licences permanentes pour qu'elles soient disponibles dans Smart Software Manager. Tous les comptes ne sont pas approuvés pour la réservation de licence permanente. Assurez-vous d'avoir l'approbation de Cisco pour cette fonctionnalité avant de tenter de la configurer.
- Demandez une licence permanente après le démarrage d'ASA virtuel; vous ne pouvez pas installer de licence permanente dans le cadre de la configuration du jour 0.

Procédure

Étape 1 (ASAv5 uniquement) Exécutez cette commande pour autoriser l'utilisation de la licence permanente ASAv5 lorsque la DRAM est de 2 Go (le minimum requis dans la version 9.13 et les versions ultérieures) :

license smart set_plr5

Étape 2 Activez la réservation de licence permanente à partir de l'interface de ligne de commande de l'ASA virtuel :

license smart reservation

Exemple :

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

Pour utiliser une licence Smart standard, utilisez la forme **no** de cette commande .

Les commandes suivantes sont supprimées :

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

Étape 3 Demandez le code de licence à saisir dans Smart Software Manager :

license smart reservation request universal

Exemple :

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
```

```
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

si vous modifiez la mémoire ou les vCPU, vous devrez renvoyer la licence actuelle et demander une nouvelle licence au nouveau niveau de modèle. La licence demandée doit correspondre à la mémoire et aux vCPU installées. Pour en savoir plus sur la vCPU et la matrice de mémoire en licence pour la réservation de licence permanente d'ASA virtuel, consultez Réservation de licence permanente pour l'ASA virtuel, à la page 91.

Pour modifier le modèle d'un ASA virtuel déjà déployé, à partir de l'hyperviseur, vous pouvez modifier les paramètres des vCPU et de la DRAM pour qu'ils correspondent aux exigences du nouveau modèle; consultez le guide de démarrage rapide d'ASA virtuel pour connaître ces valeurs. Pour afficher votre modèle actuel, utilisez la commande **show vm**.

Si vous saisissez à nouveau cette commande, le même code s'affiche, même après un rechargement. Si vous n'avez pas encore saisi ce code dans Smart Software Manager et que vous souhaitez annuler la demande, saisissez :

license smart reservation cancel

Si vous désactivez la réservation de licence permanente, toutes les demandes en attente sont annulées. Si vous avez déjà saisi le code dans Smart Software Manager, vous devez effectuer cette procédure pour appliquer la licence à l'ASA virtuel, après quoi vous pouvez renvoyer la licence si vous le souhaitez. Consultez (Facultatif) Retourner la licence permanente ASA virtuel, à la page 131.

Étape 4 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Licenses** (Licences) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Licenses** (Licences) affiche toutes les licences existantes liées à votre compte, standard et permanentes.

Étape 5 Cliquez sur **License Reservation** (Réservation de licence) et saisissez le code de l'ASA virtuel dans le champ **Reservation Request Code** (Code de demande de réservation).

Étape 6 Cliquez sur **Reserve License** (Réserver la licence).

Smart Software Manager génère un code d'autorisation. Vous pouvez télécharger le code ou le copier dans le presse-papiers. À ce stade, la licence est utilisée selon Smart Software Manager.

Si vous ne voyez pas de bouton **License Reservation** (Réservation de licence), votre compte n'est pas autorisé pour la réservation de licence permanente. Dans ce cas, vous devez désactiver la réservation de licence permanente et saisir les commandes de licence Smart normales.

Étape 7 À partir de l'interface de ligne de commande de l'ASA virtuel, exécutez la commande suivante et saisissez le code d'autorisation :

license smart reservation install *code*

Exemple :

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
INFO: ASAv platform license state is Licensed.
ciscoasa#
```

Votre ASA virtuel a maintenant une licence complète.

Étape 8 Exécutez cette commande pour enregistrer la configuration en cours d'exécution dans la configuration de démarrage afin d'éviter toute perte de configuration lors du redémarrage.

write memory

(Facultatif) Retourner la licence permanente ASA virtuel

Si vous n'avez plus besoin d'une licence permanente, par exemple, vous retirez l'ASA virtuel ou modifiez son niveau de modèle, en raison duquel il a besoin d'une nouvelle licence, vous devez officiellement retourner la licence à Smart Software Manager en utilisant cette procédure. Si vous ne suivez pas toutes les étapes, la licence reste dans un état utilisé et ne peut pas être libérée pour être utilisée ailleurs.

Procédure

Étape 1 À partir de l'interface de ligne de commande d'ASA virtuel, générez un code de retour :

license smart reservation return

Exemple :

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

L'ASA virtuel devient immédiatement sans licence et passe à l'état d'évaluation. Si vous devez afficher de nouveau ce code, ressaisissez cette commande. Notez que si vous demandez une nouvelle licence permanente (**license smart reservation request universal**) ou si vous modifiez le niveau de modèle d'ASA virtuel (en activant et en modifiant les vCPU/RAM), vous ne pouvez pas réafficher ce code. Assurez-vous de capturer le code pour terminer le retour.

Étape 2 Affichez l'identifiant universel d'appareil (UDI) ASA virtuel pour vous permettre de trouver votre instance ASA virtuel dans Smart Software Manager.

show license udi

Exemple :

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

Étape 3 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Product Instances** (Instances de produit) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Product Instances** (Instances de produit) affiche tous les produits sous licence par l'UDI.

Étape 4 Recherchez l'ASA virtuel dont vous souhaitez annuler la licence, choisissez **Actions** > **Remove (Supprimer)** et saisissez le code de retour ASA virtuel dans le champ **Reservation Return Code** (Code de retour de réservation).

La licence permanente est renvoyée vers l'ensemble disponible.

Étape 5 Cliquez sur **Remove Product Instance** (Supprimer l'instance de produit) (Supprimer la réservation).

Étape 6 Pour désactiver la réservation de licence permanente, procédez comme suit :

a) Exécutez la commande suivante pour désactiver la réservation de licence permanente :

no license smart reservation

b) Exécutez la commande suivante pour confirmer que la licence est annulée :

show license features

La sortie de la commande affiche `No active allowed` (Aucun droit actif).

Étape 7 Exécutez cette commande pour enregistrer la configuration en cours d'exécution dans la configuration de démarrage afin d'éviter toute perte de configuration lors du redémarrage.

write memory

(Facultatif) Annuler l'enregistrement de l'ASA virtuel (standard et sur site)

L'annulation de l'enregistrement de l'ASA virtuel supprime l'ASA virtuel de votre compte. Tous les droits de licence et tous les certificats de l'ASA virtuel sont supprimés. Vous souhaiterez peut-être vous désinscrire pour libérer une licence pour un nouvel ASA virtuel. Sinon, vous pouvez supprimer l'ASA virtuel du Smart Software Manager.

Remarque Si vous annulez l'enregistrement de l'ASA virtuel, il reviendra à un état de débit fortement limité après avoir rechargé l'ASA virtuel.

Procédure

Annulez l'enregistrement de ASA virtuel :

annulation de l'enregistrement de la licence Smart

L'ASA virtuel se recharge ensuite.

(Facultatif) Renouveler le certificat d'ID ou le droit de licence de l'ASA virtuel (standard et sur site)

Par défaut, le certificat d'ID est automatiquement renouvelé tous les six mois et le droit de licence est renouvelé tous les 30 jours. Vous pourriez souhaiter renouveler manuellement l'enregistrement de l'un de ces éléments si vous avez une fenêtre limitée pour l'accès Internet, ou si vous apportez des modifications de licence dans Smart Software Manager, par exemple.

Procédure

Étape 1 Renouvelez le certificat d'ID :

license smart renew id

Étape 2 Renouvelez le droit de licence :

license smart renew auth

1000/2100/3100 : configurer les licences logicielles Smart

Cette section décrit comment configurer les licences logicielles Smart pour le 1000/2100/3100. À cette fin, choisissez l'une des méthodes suivantes :

- 1000/2100/3100 : configurer les licences logicielles Smart standard, à la page 133

  Vous pouvez également (Facultatif) Annuler l'enregistrement de 1000/2100/3100 (standard et sur site), à la page 145 ou (Facultatif) Renouveler le certificat d'ID ou le droit de licence des modèles 1000/2100/3100 (standard et sur site), à la page 146.

- 1000/2100/3100 : configurer les licences Smart Software Manager sur site, à la page 138

  Vous pouvez également (Facultatif) Annuler l'enregistrement de 1000/2100/3100 (standard et sur site), à la page 145 ou (Facultatif) Renouveler le certificat d'ID ou le droit de licence des modèles 1000/2100/3100 (standard et sur site), à la page 146.

- 1000/2100/3100 : configurer la réservation de licence permanente, à la page 141

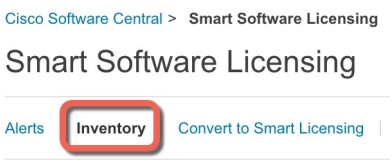
1000/2100/3100 : configurer les licences logicielles Smart standard

Cette procédure s'applique à un ASA utilisant Smart Software Manager.

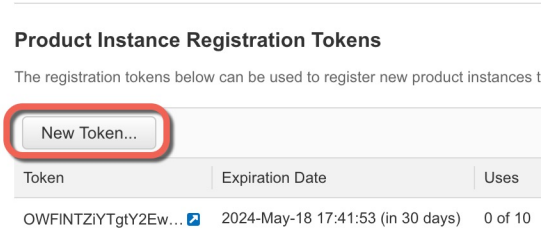
Procédure

Étape 1 Dans Cisco Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

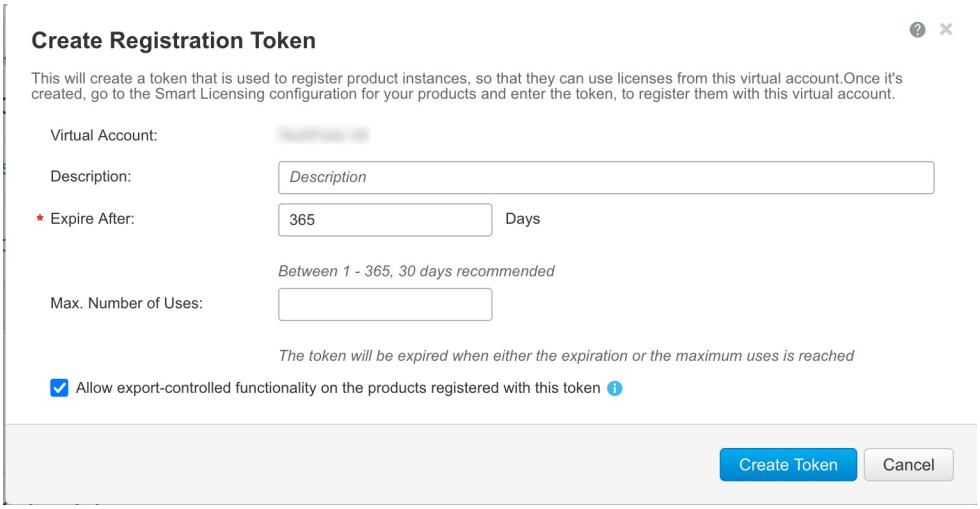
a) Cliquez sur **Inventory** (Inventaire).



b) Dans l'onglet **General** (Général), cliquez sur **New Token** (Nouveau jeton).



c) Dans la boîte de dialogue **Create Registration Token** (Créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (Créer un jeton) :



- **Description**
- **Expire After** (Expiration après) : Cisco recommande 30 jours.
- **Nombre max. d'utilisations**
- **Allow export-controlled functionality on the products registered with this token** (Autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton) : active l'indicateur de conformité à l'exportation.

Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (Jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Conservez ce jeton à portée de main pour la suite de la procédure, lorsque vous devrez enregistrer l'ASA.

Illustration 18 : Afficher le jeton

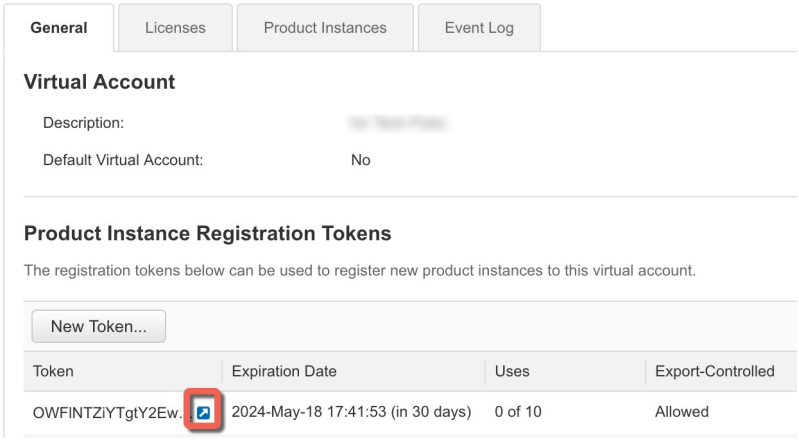
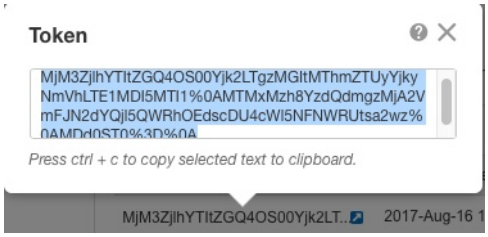


Illustration 19 : Copier le jeton



Étape 2 (Facultatif) Sur l'ASA, spécifiez l'URL du mandataire HTTP pour Call Home :

call-home

http-proxy *ip_address* **port** *port*

Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configuer l'adresse du mandataire pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Transport et Smart Call Home en général.

Remarque
Le mandataire HTTP avec l'authentification n'est pas pris en charge.

Exemple :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

Étape 3 Demandez des droits de licence sur l'ASA.

a) Entrez en mode de configuration de la licence Smart :

license smart

Exemple :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) (Firepower 1000/2100) Définissez le niveau de fonctionnalité :

feature tier standard

Seul le niveau Standard (Essentials) est disponible, cependant, vous devez l'activer dans la configuration; une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités.La licence Essentials était auparavant appelée licence Standard, et « Standard » est toujours utilisé dans l'interface de ligne de commande. Pour les modèles Secure Firewall, la licence Essentials est toujours activée et ne peut pas être désactivée.

c) Demandez la licence de contexte de sécurité.

feature context *number*

Remarque
Cette licence n'est pas prise en charge pour Firepower 1010.

Par défaut, l'ASA prend en charge 2 contextes. Vous devez donc demander le nombre de contextes souhaités moins les 2 contextes par défaut. Le nombre maximal de contextes dépend de votre modèle :

- Firepower 1120 : 5 contextes
- Firepower 1140 : 10 contextes
- Firepower 1150 : 25 contextes
- Firepower 2110 : 25 contextes
- Firepower 2120 : 25 contextes
- Firepower 2130 : 30 contextes
- Firepower 2140 : 40 contextes
- Cisco Secure Firewall 3100 : 100 contextes

Par exemple, pour utiliser le maximum de 25 contextes de Firepower 1150, saisissez 23 comme nombre de contextes. Cette valeur est ajoutée à la valeur par défaut de 2.

Exemple :

```
ciscoasa(config-smart-lic)# feature context 18
```

d) (Facultatif) (Firepower 1010) Demandez la licence Security Plus pour activer le basculement.

feature security-plus

Exemple :

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) (Facultatif) (Secure Firewall 3100) Demandez la licence d'opérateur pour l'inspection Diameter, GTP/GPRS et SCTP.

feature carrier

Exemple :

```
ciscoasa(config-smart-lic)# feature carrier
```

f) (Facultatif) Activez le cryptage renforcé. **Ne saisissez pas** cette commande si vous recevez le jeton de cryptage renforcé.

feature strong-encryption

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Remarque
Si vous saisissez cette commande, votre appareil utilisera la licence de cryptage renforcé, qu'elle soit nécessaire ou non. Donc, à moins que vous n'ayez cette licence dans votre compte, votre compte ne sera pas conforme. Étant donné que cette licence n'est pas nécessaire lors de l'utilisation du jeton de cryptage renforcé, vous pouvez accidentellement rendre votre compte non conforme sans aucun avantage.

Exemple :

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

Étape 4 Enregistrez l'ASA à l'aide du jeton que vous avez copié à l'étape 1 :

license smart register idtoken *id_token*

Exemple :

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

L'ASA s'enregistre auprès de Smart Software Manager et demande l'autorisation pour les droits de licence configurés. Le Cisco Smart Software Manager applique également la licence de cryptage renforcé (3DES/AES) si votre compte le permet. Utilisez la commande **show license summary** pour vérifier l'état et l'utilisation de la licence.

Exemple :

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC
```

```
License Usage:
  License                Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP1010-ASA-Std)                    1 AUTHORIZED
```

1000/2100/3100 : configurer les licences Smart Software Manager sur site

Cette procédure s'applique à un ASA utilisant Smart Software Manager sur site.

Avant de commencer

- Téléchargez le fichier OVA Smart Software Manager sur site à partir de Cisco.com, installez-le et configurez-le sur un serveur VMwareESXi. Pour en savoir plus, consultez la *fiche technique de Cisco Smart Software Manager sur site*.
- Téléchargez le groupe de confiance CA de chiffrement avant de placer l'appareil dans un réseau isolé. Ce groupe de confiance est normalement téléchargé automatiquement, mais peut être obsolète dans un réseau isolé :

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

Procédure

Étape 1 Demandez un jeton d'enregistrement sur le serveur Smart Software Manager sur site.

Étape 2 (Facultatif) Sur l'ASA, spécifiez l'URL du mandataire HTTP pour Call Home :

call-home

http-proxy *ip_address* **port** *port*

Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configuer l'adresse du mandataire pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Transport et Smart Call Home en général.

Remarque
Le mandataire HTTP avec l'authentification n'est pas pris en charge.

Exemple :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

Étape 3 Changez l'URL du serveur de licence pour accéder à Smart Software Manager sur site.

call-home

profile License

destination address http https://*on-prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

Exemple :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile) destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

Étape 4 Demandez des droits de licence sur l'ASA.

a) Entrez en mode de configuration de la licence Smart :

license smart

Exemple :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) (Firepower 1000/2100) Définissez le niveau de fonctionnalité :

feature tier standard

Seul le niveau Standard (Essentials) est disponible, cependant, vous devez l'activer dans la configuration; une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités.La licence Essentials était auparavant appelée licence Standard, et « Standard » est toujours utilisé dans l'interface de ligne de commande. Pour les modèles Secure Firewall, la licence Essentials est toujours activée et ne peut pas être désactivée.

c) (Facultatif) Demandez la licence de contexte de sécurité.

feature context *number*

Remarque
Cette licence n'est pas prise en charge pour Firepower 1010.

Par défaut, l'ASA prend en charge 2 contextes. Vous devez donc demander le nombre de contextes souhaités moins les 2 contextes par défaut. Le nombre maximal de contextes dépend de votre modèle :

- Firepower 1120 : 5 contextes
- Firepower 1140 : 10 contextes
- Firepower 1150 : 25 contextes
- Firepower 2110 : 25 contextes
- Firepower 2120 : 25 contextes
- Firepower 2130 : 30 contextes
- Firepower 2140 : 40 contextes
- Cisco Secure Firewall 3100 : 100 contextes

Par exemple, pour utiliser le maximum de 25 contextes de Firepower 1150, saisissez 23 comme nombre de contextes. Cette valeur est ajoutée à la valeur par défaut de 2.

Exemple :

```
ciscoasa(config-smart-lic)# feature context 18
```

d) (Facultatif) (Firepower 1010) Demandez la licence Security Plus pour activer le basculement.

feature security-plus

Exemple :

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) (Facultatif) (Secure Firewall 3100) Demandez la licence d'opérateur pour l'inspection Diameter, GTP/GPRS et SCTP.

feature carrier

Exemple :

```
ciscoasa(config-smart-lic)# feature carrier
```

f) (Facultatif) Activez le cryptage renforcé. **Ne saisissez pas** cette commande si vous recevez le jeton de cryptage renforcé.

feature strong-encryption

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Remarque
Si vous saisissez cette commande, votre appareil utilisera la licence de cryptage renforcé, qu'elle soit nécessaire ou non. Donc, à moins que vous n'ayez cette licence dans votre compte, votre compte ne sera pas conforme. Étant donné que cette licence n'est pas nécessaire lors de l'utilisation du jeton de cryptage renforcé, vous pouvez accidentellement rendre votre compte non conforme sans aucun avantage.

Exemple :

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

Étape 5 Enregistrez l'ASA à l'aide du jeton que vous avez demandé à l'étape 1 :

license smart register idtoken *id_token*

Exemple :

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

L'ASA s'enregistre auprès du serveur Smart Software Manager sur site et demande l'autorisation pour les droits de licence configurés. Le serveur Smart Software Manager sur site applique également la licence de cryptage renforcé (3DES/AES) si votre compte le permet. Utilisez la commande **show license summary** pour vérifier l'état et l'utilisation de la licence.

Exemple :

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP1010-ASA-Std)                    1 AUTHORIZED
```

1000/2100/3100 : configurer la réservation de licence permanente

Vous pouvez attribuer une licence permanente à un Firepower 1000/2100, Secure Firewall . Cette section décrit également comment restituer une licence si vous retirez l'ASA.

Procédure

Étape 1 Installer la licence permanente 1000/2100/3100, à la page 141.

Étape 2 (Facultatif) Renvoyez la licence permanente 1000/2100/3100, à la page 144.

Installer la licence permanente 1000/2100/3100

Pour les ASA qui n'ont pas d'accès Internet, vous pouvez demander une licence permanente auprès de Smart Software Manager. La licence permanente active toutes les fonctionnalités : Essentials licence avec un nombre maximum de contextes de sécurité.

Remarque Pour la réservation de licence permanente, vous devez retourner la licence avant de désactiver l'ASA. Si vous ne retournez pas officiellement la licence, la licence reste dans un état usagé et ne peut pas être réutilisée pour un nouvel ASA. Consultez (Facultatif) Renvoyez la licence permanente 1000/2100/3100, à la page 144.

Avant de commencer

Achetez des licences permanentes de sorte qu'elles soient disponibles dans Smart Software Manager. Tous les comptes ne sont pas approuvés pour la réservation de licence permanente. Assurez-vous d'avoir l'approbation de Cisco pour cette fonctionnalité avant de tenter de la configurer.

Procédure

Étape 1 Activez la réservation de licence permanente au niveau de l'interface de ligne de commande de l'ASA :

license smart reservation

Exemple :

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

Étape 2 Demandez le code de licence à saisir dans Smart Software Manager :

license smart reservation request universal

Exemple :

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

Si vous saisissez à nouveau cette commande, le même code s'affiche, même après un rechargement. Si vous n'avez pas encore saisi ce code dans Smart Software Manager et que vous souhaitez annuler la demande, saisissez :

license smart reservation cancel

Si vous désactivez la réservation de licence permanente, toutes les demandes en attente sont annulées. Si vous avez déjà saisi le code dans Smart Software Manager, vous devez effectuer cette procédure pour appliquer la licence à l'ASA, après quoi vous pouvez renvoyer la licence si vous le souhaitez. Consultez (Facultatif) Renvoyez la licence permanente 1000/2100/3100, à la page 144.

Étape 3 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Licenses** (Licences) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Licenses** (Licences) affiche toutes les licences existantes liées à votre compte, standard et permanentes.

Étape 4 Cliquez sur **License Reservation** (Réservation de licence) et saisissez le code ASA dans la zone. Cliquez sur **Reserve License** (Réserver la licence).

Smart Software Manager génère un code d'autorisation. Vous pouvez télécharger le code ou le copier dans le presse-papiers. À ce stade, la licence est utilisée selon Smart Software Manager.

Si vous ne voyez pas de bouton **License Reservation** (Réservation de licence), votre compte n'est pas autorisé pour la réservation de licence permanente. Dans ce cas, vous devez désactiver la réservation de licence permanente et saisir les commandes de licence Smart normales.

Étape 5 Sur l'ASA, saisissez le code d'autorisation :

license smart reservation install *code*

Exemple :

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

Étape 6 Demandez des droits de licence sur l'ASA.

Remarque
Bien que la licence permanente permette l'utilisation complète de toutes les licences, vous devez toujours activer les droits dans la configuration ASA pour que l'ASA sache qu'il peut les utiliser.

a) Entrez en mode de configuration de la licence Smart :

license smart

Exemple :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) (Firepower 1000/2100) Définissez le niveau de fonctionnalité :

feature tier standard

Seul le niveau Standard (Essentials) est disponible, cependant, vous devez l'activer dans la configuration; une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités.La licence Essentials était auparavant appelée licence Standard, et « Standard » est toujours utilisé dans l'interface de ligne de commande. Pour les modèles Secure Firewall, la licence Essentials est toujours activée et ne peut pas être désactivée.

c) (Facultatif) Activez la licence de contexte de sécurité.

feature context *number*

Remarque
Cette licence n'est pas prise en charge pour Firepower 1010.

Par défaut, l'ASA prend en charge 2 contextes. Vous devez donc activer le nombre de contextes souhaités moins les 2 contextes par défaut. Comme la licence permanente autorise le nombre maximum, vous pouvez activer le nombre maximum pour votre modèle. Le nombre maximal de contextes dépend de votre modèle :

- Firepower 1120 : 5 contextes
- Firepower 1140 : 10 contextes
- Firepower 1150 : 25 contextes
- Firepower 2110 : 25 contextes
- Firepower 2120 : 25 contextes
- Firepower 2130 : 30 contextes
- Firepower 2140 : 40 contextes

- Cisco Secure Firewall 3100 : 100 contextes

Par exemple, pour utiliser le maximum de 25 contextes de Firepower 1150, saisissez 23 comme nombre de contextes. Cette valeur est ajoutée à la valeur par défaut de 2.

Exemple :

```
ciscoasa(config-smart-lic)# feature context 18
```

d) (Facultatif) (Firepower 1010) Activez la licence Security Plus pour activer le basculement.

feature security-plus

Exemple :

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) (Facultatif) (Secure Firewall 3100) Activez la licence d'opérateur pour l'inspection Diameter, GTP/GPRS et SCTP.

feature carrier

Exemple :

```
ciscoasa(config-smart-lic)# feature carrier
```

f) (Facultatif) Activez le cryptage renforcé. **Ne saisissez pas** cette commande si vous recevez le jeton de cryptage renforcé.

feature strong-encryption

Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Remarque
Si vous saisissez cette commande, votre appareil utilisera la licence de cryptage renforcé, qu'elle soit nécessaire ou non. Donc, à moins que vous n'ayez cette licence dans votre compte, votre compte ne sera pas conforme. Étant donné que cette licence n'est pas nécessaire lors de l'utilisation du jeton de cryptage renforcé, vous pouvez accidentellement rendre votre compte non conforme sans aucun avantage.

Exemple :

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

(Facultatif) Renvoyez la licence permanente 1000/2100/3100

Si vous n'avez plus besoin d'une licence permanente (par exemple, vous retirez un ASA), vous devez officiellement renvoyer la licence à Smart Software Manager en utilisant cette procédure. Si vous ne suivez

pas toutes les étapes, la licence reste dans un état utilisé et ne peut pas être libérée facilement pour être utilisée ailleurs.

Procédure

Étape 1 Sur l'ASA, générez un code de retour :

license smart reservation return

Exemple :

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

L'ASA devient immédiatement sans licence et passe à l'état d'évaluation. Si vous devez afficher de nouveau ce code, ressaisissez cette commande. Notez que si vous demandez une nouvelle licence permanente (**license smart reservation request universal**), vous ne pouvez pas réafficher ce code. Assurez-vous de capturer le code pour terminer le retour. Si la période d'évaluation a expiré, l'ASA passe à un état expiré. Pour en savoir plus sur les états de non-conformité, consultez État de non-conformité, à la page 170.

Étape 2 Affichez l'identifiant universel d'appareil (UDI) de l'ASA pour vous permettre de trouver votre instance ASA dans Smart Software Manager.

show license udi

Exemple :

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

Étape 3 Accédez à l'écran Smart Software Manager Inventory (Inventaire de Smart Software Manager), puis cliquez sur l'onglet **Product Instances** (Instances de produit) :

https://software.cisco.com/#SmartLicensing-Inventory

L'onglet **Product Instances** (Instances de produit) affiche tous les produits sous licence par l'UDI.

Étape 4 Recherchez l'ASA dont vous souhaitez annuler la licence, choisissez **Actions** > **Remove (Supprimer)** et saisissez le code de retour de l'ASA dans la zone. Cliquez sur **Remove Product Instance** (Supprimer l'instance de produit).

La licence permanente est renvoyée vers l'ensemble disponible.

(Facultatif) Annuler l'enregistrement de 1000/2100/3100 (standard et sur site)

L'annulation de l'enregistrement de l'ASA supprime l'ASA de votre compte. Tous les droits de licence et tous les certificats de l'ASA sont supprimés. Vous souhaiterez peut-être vous désinscrire pour libérer une licence pour un nouvel ASA. Sinon, vous pouvez supprimer l'ASA du Smart Software Manager.

Procédure

Annulez l'enregistrement de l'ASA :

annulation de l'enregistrement de la licence Smart

(Facultatif) Renouveler le certificat d'ID ou le droit de licence des modèles 1000/2100/3100 (standard et sur site)

Par défaut, le certificat d'ID est automatiquement renouvelé tous les six mois et le droit de licence est renouvelé tous les 30 jours. Vous pourriez souhaiter renouveler manuellement l'enregistrement de l'un de ces éléments si vous avez une fenêtre limitée pour l'accès Internet, ou si vous apportez des modifications de licence dans Smart Software Manager, par exemple.

Procédure

Étape 1 Renouvelez le certificat d'ID :

license smart renew id

Étape 2 Renouvelez le droit de licence :

license smart renew auth

Firepower 4100/9300 : configurer les licences logicielles Smart

Cette procédure s'applique pour un châssis utilisant Smart Software Manager, Smart Software Manager sur site ou pour la réservation de licence permanente; consultez le guide de configuration FXOS pour configurer votre méthode en tant que condition préalable.

Pour la réservation de licence permanente, la licence active toutes les fonctionnalités : le niveau standard avec le nombre maximum de contextes de sécurité et la licence de l'opérateur. Cependant, pour que l'ASA sache utiliser ces fonctionnalités, vous devez les activer sur l'ASA.

Avant de commencer

Pour une grappe ASA, vous devez accéder à l'unité de contrôle pour la configuration. Consultez le Firewall Chassis Manager pour voir quelle unité est l'unité de contrôle. Vous pouvez également vérifier à partir de l'interface de ligne de commande de l'ASA, comme le montre cette procédure.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande Châssis Firepower 4100/9300 (console ou SSH), puis connectez-vous à l'ASA :

connect module *slot* **console connect asa**

Exemple :

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

La prochaine fois que vous vous connecterez à la console de l'ASA, vous accéderez directement à l'ASA; vous n'aurez pas besoin de saisir à nouveau **connect asa**.

Pour une grappe ASA, il vous suffit d'accéder à l'unité de contrôle pour la configuration des licences et les autres configurations. Généralement, l'unité de contrôle se trouve dans le logement 1, vous devez donc d'abord vous connecter à ce module.

Étape 2 Au niveau de l'interface de ligne de commande de l'ASA, entrez en mode de configuration globale. Par défaut, le mot de passe d'activation est une valeur vide, sauf si vous l'avez défini lors du déploiement du périphérique logique, mais vous êtes invité à modifier le mot de passe la première fois que vous entrez la commande **enable**.

enable configure terminal

Exemple :

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa# configure terminal
asa(config)#
```

Étape 3 Si nécessaire, pour une grappe ASA, confirmez que cette unité est l'unité de contrôle :

show cluster info

Exemple :

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
```

```
  Version : 9.5(2)
  Serial No.: P3000000001
  CCL IP : 127.2.1.2
  CCL MAC : 000b.fcf8.c162
  Last join : 19:13:11 UTC Sep 23 2015
  Last leave: N/A
Unit "unit-1-3" in state MASTER
  ID : 2
  Version : 9.5(2)
  Serial No.: JAB0815R0JY
  CCL IP : 127.2.1.3
  CCL MAC : 000f.f775.541e
  Last join : 19:13:20 UTC Sep 23 2015
  Last leave: N/A
```

Si une autre unité est l'unité de contrôle, quittez la connexion et connectez-vous à l'unité appropriée. Voir ci-dessous pour savoir comment quitter la connexion.

Étape 4 Entrez en mode de configuration de la licence Smart :

license smart

Exemple :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

Étape 5 Définissez le niveau de fonctionnalité :

feature tier standard

Seul le niveau standard est disponible. Une licence de niveau est une condition préalable à l'ajout d'autres licences de fonctionnalités. Vous devez avoir suffisamment de licences de niveau dans votre compte. Sinon, vous ne pouvez pas configurer d'autres licences de fonctionnalités ou des fonctionnalités nécessitant des licences.

Étape 6 Demandez une ou plusieurs des fonctionnalités suivantes :

- Opérateur (inspection GTP/GPRS, Diameter et SCTP)

  feature carrier

- Contextes de sécurité

  feature context *<1-248>*

  Pour la réservation de licence permanente, vous pouvez spécifier le nombre de contextes maximum (248).

- Strong Encryption (cryptage renforcé) (normes 3DES/AES)

  feature strong-encryption

  Cette licence n'est pas requise si vous recevez le jeton de cryptage renforcé de Smart Software Manager. Cependant, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité active demande cette licence et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.

Exemple :

```
ciscoasa(config-smart-lic)# feature carrier
ciscoasa(config-smart-lic)# feature context 50
```

Étape 7 Pour quitter la console de l'ASA, entrez ~ à l'invite pour quitter l'application Telnet. Entrez **quit** pour revenir à l'interface de ligne de commande du superviseur.

Licences par modèle

Cette section répertorie les droits de licence disponibles pour le module de sécurité ASAv et Châssis Firepower 4100/9300 ASA.

ASA virtuel

Lorsque vous définissez le niveau de débit dans la configuration ASA à l'aide de la commande **throughput level**, cela détermine la licence demandée à Smart Software Manager. Consultez la relation suivante entre niveau de débit et licence :

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

Le niveau de débit détermine également les sessions de mandataire TLS et Secure Client (services client sécurisés) maximum. Cependant, un profil de mémoire ASA virtuel inférieur limitera votre nombre réel de sessions. Par conséquent, pour déterminer vos sessions, vous devez vérifier le niveau de débit et la mémoire installée.

La mémoire de votre ASA virtuel détermine le nombre maximum de connexions et de VLAN simultanés de pare-feu et n'est pas déterminée par le niveau de débit.

Le tableau suivant présente les fonctionnalités sous licence de la gamme ASA virtuel.

Licences	Description
Licences d'autorisation	

Licences	Description
Niveau de débit	Vous définissez le niveau de débit dans la configuration ASA à l'aide de la commande **throughput level**. Ce niveau détermine la licence dont vous avez besoin. 100 M : ASAv5 1 G : ASAv10 2 G : ASAv30 10 G : ASAv50 20 G : ASAv100
Licences de pare-feu	
Filtre de trafic de réseau de zombies	Activé
Connexions de pare-feu, simultanées	Les connexions de pare-feu sont déterminées par la mémoire d'ASA virtuel. De 2 Go à 7,9 Go : 100 000 De 8 Go à 15,9 Go : 500 000 De 16 Go à 31,9 Go : 2 000 000 32 Go à 64 Go : 4 000 000
Transporteur	Activé

Licences	Description
Nombre total de sessions de mandataire TLS	Les sessions de mandataire TLS sont déterminées par le niveau de débit et la mémoire d'ASA virtuel. Débit de 100 M + toute mémoire : 500 Débit de 1 G + toute mémoire : 500 Débit de 2 G : • Mémoire de 2 Go à 7,9 Go : 500 • Mémoire de 8 Go+ : 1000 Débit de 10 G : • Mémoire de 2 Go à 7,9 Go : 500 • Mémoire de 8 Go à 15,9 Go : 1 000 • Mémoire de 16 Go+ : 10 000 Débit de 20 G : • Mémoire de 2 Go à 7,9 Go : 500 • Mémoire de 8 Go à 15,9 Go : 1 000 • Mémoire de 16 Go à 31,9 Go : 10 000 • Mémoire de 32 Go+ : 20 000
Licences VPN	

Licences	Description	
Homologues Secure Client (services client sécurisés)	Sans licence	Les homologues Secure Client (services client sécurisés) sont déterminés par le niveau de débit et la mémoire d'ASA virtuel. *Licence Secure Client Advantage ou Secure Client Premier facultative, maximums :* *Débit de 100 M + toute mémoire : 50* *Débit de 1 Go + toute mémoire : 250* *Débit de 2 G :* • *Mémoire de 2 Go à 7,9 Go : 250* • *Mémoire de 8 Go+ : 750* *Débit de 10 G :* • *Mémoire de 2 Go à 7,9 Go : 250* • *Mémoire de 8 Go à 15,9 Go : 750* • *Mémoire de 16 Go+ : 10 000* *Débit de 20 G :* • *Mémoire de 2 Go à 7,9 Go : 250* • *Mémoire de 8 Go à 15,9 Go : 750* • *De 16 Go à 31,9 Go : 10 000* • *Mémoire de 32 Go+ : 20 000*

Licences	Description
Autres homologues VPN	**Remarque** Les autres homologues VPN sont déterminés par le niveau de débit et la mémoire d'ASA virtuel. Débit de 100 M + toute mémoire : 50 Débit de 1 Go + toute mémoire : 250 Débit de 2 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go+ : 750 Débit de 10 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • Mémoire de 16 Go+ : 10 000 Débit de 20 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • De 16 Go à 31,9 Go : 10 000 • Mémoire de 32 Go+ : 20 000

Licences	Description
Total des homologues VPN, tous types combinés	**Remarque** Le nombre total d'homologues VPN est déterminé par le niveau de débit et la mémoire d'ASA virtuel. Débit de 100 M + toute mémoire : 50 Débit de 1 Go + toute mémoire : 250 Débit de 2 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go+ : 750 Débit de 10 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • Mémoire de 16 Go+ : 10 000 Débit de 20 G : • Mémoire de 2 Go à 7,9 Go : 250 • Mémoire de 8 Go à 15,9 Go : 750 • De 16 Go à 31,9 Go : 10 000 • Mémoire de 32 Go+ : 20 000
Licences générales	
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte
Basculement	Actif/Veille
Contextes de sécurité	Aucune assistance
Mise en grappe	Activé
Nombre maximum de VLAN	Les VLAN sont déterminés par la mémoire d'ASA virtuel. De 2 Go à 7,9 Go—50 De 8 Go à 15,9 Go—200 De 16 Go à 31,9 Go—1 024 De 32 Go à 64 Go—1 024

Firepower 1010

Le tableau suivant présente les fonctionnalités sous licence du Firepower 1010.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	100 000	
Transporteur	Aucune assistance. Bien que les cartes d'inspection SCTP ne soient pas prises en charge, l'inspection avec état SCTP à l'aide d'ACL est prise en charge.	
Nombre total de sessions de mandataire TLS	4 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum : 75*
Autres homologues VPN	75	
Total des homologues VPN, tous types combinés	75	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Security Plus (basculement, équilibrage de charges VPN)	Désactivé	*Facultatif*
Contextes de sécurité	Aucune assistance.	
Mise en grappe	Aucune assistance.	
Nombre maximum de VLAN	60	

Gamme Firepower 1100

Le tableau suivant présente les fonctionnalités sous licence de la gamme Firepower 1100.

Licences	Licence Essentials
Licences de pare-feu	
Filtre de trafic de réseau de zombies	Aucune prise en charge.

Licences	Licence Essentials	
Connexions de pare-feu, simultanées	Firepower 1120 : 200 000 Firepower 1140 : 400 000 Firepower 1150 : 600 000	
Transporteur	Aucune assistance. Bien que les cartes d'inspection SCTP ne soient pas prises en charge, l'inspection avec état SCTP à l'aide d'ACL est prise en charge.	
Nombre total de sessions de mandataire TLS	Firepower 1120 : 4 000 Firepower 1140 : 8 000 Firepower 1150 : 8 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum :* *Firepower 1120 : 150* *Firepower 1140 : 400* *Firepower 1150 : 800*
Autres homologues VPN	Firepower 1120 : 150 Firepower 1140 : 400 Firepower 1150 : 800	
Total des homologues VPN, tous types combinés	Firepower 1120 : 150 Firepower 1140 : 400 Firepower 1150 : 800	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	2	*Licence facultative, maximum :* *Firepower 1120 : 5* *Firepower 1140 : 10* *Firepower 1150 : 25*
Mise en grappe	Aucune assistance.	
Nombre maximum de VLAN	1024	

Firepower Série 2100

Le tableau suivant présente les fonctionnalités sous licence de la gamme Firepower 2100.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	Firepower 2110 : 1 000 000 Firepower 2120 : 1 500 000 Firepower 2130 : 2 000 000 Firepower 2140 : 3 000 000	
Transporteur	Aucune assistance. Bien que les cartes d'inspection SCTP ne soient pas prises en charge, l'inspection avec état SCTP à l'aide d'ACL est prise en charge.	
Nombre total de sessions de mandataire TLS	Firepower 2110 : 4 000 Firepower 2120 : 8 000 Firepower 2130 : 8 000 Firepower 2140 : 10 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum :* *Firepower 2110 : 1 500* *Firepower 2120 : 3 500* *Firepower 2130 : 7 500* *Firepower 2140 : 10 000*
Autres homologues VPN	Firepower 2110 : 1 500 Firepower 2120 : 3 500 Firepower 2130 : 7 500 Firepower 2140 : 10 000	
Total des homologues VPN, tous types combinés	Firepower 2110 : 1 500 Firepower 2120 : 3 500 Firepower 2130 : 7 500 Firepower 2140 : 10 000	

Licences	Licence Essentials	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	2	*Licence facultative, maximum :* *Firepower 2110 : 25* *Firepower 2120 : 25* *Firepower 2130 : 30* *Firepower 2140 : 40*
Mise en grappe	Aucune assistance.	
Nombre maximum de VLAN	1024	

Gamme Secure Firewall 3100

Le tableau suivant présente les fonctionnalités sous licence de la gamme Secure Firewall 3100.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	Secure Firewall 3105 : 2 000 000 Secure Firewall 3110 : 2 000 000 Secure Firewall 3120 : 4 000 000 Secure Firewall 3130 : 6 000 000 Secure Firewall 3140 : 10 000 000	
Transporteur	Désactivé	*Licence facultative : opérateur*
Nombre total de sessions de mandataire TLS	Secure Firewall 3105 : 10 000 Secure Firewall 3110 : 10 000 Secure Firewall 3120 : 15 000 Secure Firewall 3130 : 15 000 Secure Firewall 3140 : 15 000	
Licences VPN		

Licences	Licence Essentials	
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement , maximum :* *Secure Firewall 3105 : 3 000* *Secure Firewall 3110 : 3 000* *Secure Firewall 3120 : 7 000* *Secure Firewall 3130 : 15 000* *Secure Firewall 3140 : 20 000*
Autres homologues VPN	Secure Firewall 3105 : 3 000 Secure Firewall 3110 : 3 000 Secure Firewall 3120 : 7 000 Secure Firewall 3130 : 15 000 Secure Firewall 3140 : 20 000	
Total des homologues VPN, tous types combinés	Secure Firewall 3105 : 3 000 Secure Firewall 3110 : 3 000 Secure Firewall 3120 : 7 000 Secure Firewall 3130 : 15 000 Secure Firewall 3140 : 20 000	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	2	*Licence facultative, maximum : 100*
Mise en grappe	Activé	
Nombre maximum de VLAN	1024	

Firepower 4100

Le tableau suivant présente les fonctionnalités sous licence du Firepower 4100.

Licences	Licence Essentials
Licences de pare-feu	
Filtre de trafic de réseau de zombies	Aucune prise en charge.

Licences	Licence Essentials	
Connexions de pare-feu, simultanées	Firepower 4112 : 10 000 000 Firepower 4115 : 15 000 000 Firepower 4125 : 25 000 000 Firepower 4145 : 40 000 000	
Transporteur	Désactivé	*Licence facultative : opérateur*
Nombre total de sessions de mandataire TLS	15 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement :* *Firepower 4112 : 10 000* *Firepower 4115 : 15 000* *Firepower 4125 : 20 000* *Firepower 4145 : 20 000*
Autres homologues VPN	Firepower 4112 : 10 000 Firepower 4115 : 15 000 Firepower 4125 : 20 000 Firepower 4145 : 20 000	
Total des homologues VPN, tous types combinés	Firepower 4112 : 10 000 Firepower 4115 : 15 000 Firepower 4125 : 20 000 Firepower 4145 : 20 000	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	10	*Licence facultative : maximum de 250*
Mise en grappe	Activé	
Nombre maximum de VLAN	1024	

Firepower 9300

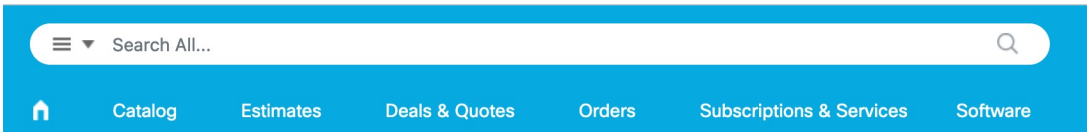
Le tableau suivant présente les fonctionnalités sous licence du Firepower 9300.

Licences	Licence Essentials	
Licences de pare-feu		
Filtre de trafic de réseau de zombies	Aucune prise en charge.	
Connexions de pare-feu, simultanées	Firepower 9300 SM-56 : 60 000 000 Firepower 9300 SM-48 : 60 000 000 Firepower 9300 SM-40 : 55 000 000	
Carrier (exploitant)	Désactivé	*Licence facultative : opérateur*
Nombre total de sessions de mandataire TLS	15 000	
Licences VPN		
Homologues Secure Client (services client sécurisés)	Sans licence	*Licence facultative Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement : 20 000 maximum*
Autres homologues VPN	20 000	
Total des homologues VPN, tous types combinés	20 000	
Licences générales		
Chiffrement	De base (DES) ou renforcé (3DES/AES), selon les paramètres de conformité en matière d'exportation du compte	
Contextes de sécurité	10	*Licence facultative : maximum de 250*
Mise en grappe	Activé	
Nombre maximum de VLAN	1024	

PID de licence par modèle

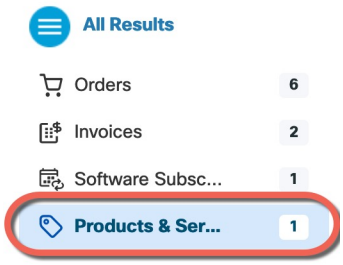
Lorsque vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte de gestion des licences Smart Software. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ **Search All** (tout rechercher) de Cisco Commerce Workspace.

Illustration 20 : Recherche de licences



Choisissez des **produits et services** dans les résultats.

Illustration 21 : Résultats



PID ASA virtuel

ASA virtuel PID de Smart Software Manager standard et sur site :

- Licence ASAv5—L-ASAV5S-K9=
- Licence ASAv10—L-ASAV10S-K9=
- Licence ASAv30—L-ASAV30S-K9=
- Licence ASAv50—L-ASAV50S-K9=
- Licence ASAv100—L-ASAV100S-1Y=
- Licence ASAv100—L-ASAV100S-3Y=
- Licence ASAv100—L-ASAV100S-5Y=

Remarque L'ASAv100 est une licence par abonnement, disponible pour 1 an, 3 ans ou 5 ans.

ASA virtuel PID de réservation de licence permanente :

La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

- Licence ASAv5—L-ASAV5SR-K9=
- Licence ASAv10—L-ASAV10SR-K9=
- Licence ASAv30—L-ASAV30SR-K9=

- Licence ASAv50—L-ASAV50SR-K9=
- Licence ASAv100—L-ASAV100SR-K9=

Numéros d'ID de produits Firepower 1010

Numéros de produit standard et sur site de Firepower 1010 Smart Software Manager :

- Essentials—L-FPR1000-ASA=. Nécessaire.
- Security Plus—L-FPR1010-SEC-PL=. La licence Security Plus permet le basculement.
- Cryptage renforcé (3DES/AES)—L-FPR1K-ENC-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.

PID de réservation de licence permanente Firepower 1010 :

La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

- L-FPR1K-ASA-BPU =

Numéros d'ID de produits pour l'appareil Firepower 1100

PID standard et sur site de Firepower 1100 Smart Software Manager :

- Essentials—L-FPR1000-ASA=. Nécessaire.
- 5 licences de contexte — L-FPR1K-ASASC-5=. Les licences de contexte sont cumulatives; achetez plusieurs licences.
- 10 licences de contexte — L-FPR1K-ASASC-10=. Les licences de contexte sont cumulatives; achetez plusieurs licences.
- Cryptage renforcé (3DES/AES)—L-FPR1K-ENC-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.

PID de réservation de licence permanente Firepower 1100 :

La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

- L-FPR1K-ASA-BPU =

PID Firepower 2100

PID standard et sur site de Firepower 2100 Smart Software Manager :

- Essentials—L-FPR2100-ASA=. Nécessaire.

- 5 licences de contexte — L-FPR2K-ASASC-5=. Les licences de contexte sont cumulatives; achetez plusieurs licences.
- 10 licences de contexte — L-FPR2K-ASASC-10=. Les licences de contexte sont cumulatives; achetez plusieurs licences.
- Cryptage renforcé (3DES/AES) — L-FPR2K-ENC-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.

PID de réservation de licence permanente Firepower 2100 :

La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

- L-FPR2K-ASA-BPU =

PID Secure Firewall 3100

PID standard et sur site de Secure Firewall 3100 Smart Software Manager :

- Essentials — *automatiquement incluse*.
- 5 licences de contexte — L-FPR3K-ASASC-5=. Les licences de contexte sont cumulatives; achetez plusieurs licences.
- 10 licences de contexte — L-FPR3K-ASASC-10=. Les licences de contexte sont cumulatives; achetez plusieurs licences.
- Opérateur (Diameter, GTP/GPRS, M3UA, SCTP)— L-FPR3K-ASA-CAR=
- Licence de cryptage renforcé (3DES/AES) — L-FPR3K-ENC-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.

PID de réservation de licence permanente Firepower 3100 :

La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

- L-FPR3K-ASA-BPU =

PID Firepower 4100

PID standard et sur site de Firepower 4100 Smart Software Manager :

- Essentials—L-FPR4100-ASA=. Nécessaire.
- 10 licences de contexte — L-FPR3K-ASASC-10=. Les licences de contexte sont cumulatives; achetez plusieurs licences.
- 230 licences de contexte — L-FPR4K-ASASC-230 =. Les licences de contexte sont cumulatives; achetez plusieurs licences.

- 250 licences de contexte — L-FPR4K-ASASC-250 =. Les licences de contexte sont cumulatives; achetez plusieurs licences.
- Opérateur (Diameter, GTP/GPRS, M3UA, SCTP)— L-FPR4K-ASA-CAR=
- Cryptage renforcé (3DES/AES) — L-FPR3K-ENC-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.

PID de réservation de licence permanente Firepower 4100 :

La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

- L-FPR4K-ASA-BPU =

Numéros d'ID de produits pour l'appareil Firepower 9300

PID standard et sur site de Firepower 9300 Smart Software Manager :

- Essentials—L-F9K-ASA=. Nécessaire.
- 10 licences de contexte — L-F9K-ASA-SC-10=. Les licences de contexte sont cumulatives; achetez plusieurs licences.
- Opérateur (Diameter, GTP/GPRS, M3UA, SCTP)— L-F9K-ASA-CAR=
- Cryptage renforcé (3DES/AES) — L-F9K-ASA-ENCR-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.

PID de réservation de licence permanente Firepower 9300 :

La licence permanente comprend toutes les fonctionnalités disponibles, y compris la licence de cryptage renforcé (3DES/AES), si votre compte est admissible. Les fonctionnalités Secure Client (services client sécurisés) sont également activées au maximum de la plateforme, selon votre achat de la licence Secure Client (services client sécurisés) qui vous permet d'utiliser Secure Client (services client sécurisés) (voir LicencesSecure Client Advantage , Secure Client Premieret VPN client sécurisé uniquement , à la page 97).

- L-FPR9K-ASA-BPU =

Supervision des licences logicielles Smart

Vous pouvez superviser les fonctionnalités, l'état et le certificat de la licence, et activer les messages de débogage.

Affichage de votre licence actuelle

Consultez les commandes suivantes pour afficher votre licence :

- **show license features**

  L'exemple suivant montre l'ASA avec uniquement une licence Essentials :

```
ciscoasa# show license features
Serial Number:  JAD254312UA
Export Compliant: YES

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 512
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 2
Carrier                           : Disabled
AnyConnect Premium Peers          : 150
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 150
Total VPN Peers                   : 150
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 320
Cluster                           : Disabled
```

Affichage de l'état de la licence Smart

Consultez les commandes suivantes pour afficher l'état de la licence :

- **show license all**

  Affiche l'état des licences logicielles Smart, la version de Smart Agent, les renseignements de l'UDI, l'état de Smart Agent, l'état de conformité globale, l'état des droits, les renseignements sur le certificat de licence et les tâches Smart Agent planifiées.

  L'exemple suivant montre une licence ASA virtuel :

```
ciscoasa# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 21 21:17:35 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 21 21:17:35 2015 UTC
  Next Communication Attempt: Sep 24 00:44:10 2015 UTC
  Communication Deadline: Dec 20 21:14:33 2015 UTC
```

```
License Usage
==============

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
===================
UDI: PID:ASAv,SN:9AHV3KJBEKE

Agent Version
=============
Smart Agent for Licensing: 1.6_reservation/36
```

- **show license status**

  Affiche l'état de la licence Smart.

  L'exemple suivant montre l'état de l'ASA virtuel à l'aide d'une licence logicielle Smart standard :

```
ciscoasa# show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 23 01:41:26 2015 UTC
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC
  Communication Deadline: Dec 22 01:38:25 2015 UTC
```

  L'exemple suivant montre l'état de l'ASA virtuel à l'aide de la réservation de licence permanente :

```
ciscoasa# show license status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jan 28 16:42:45 2016 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Jan 28 16:42:45 2016 UTC

Licensing HA configuration error:
```

```
    No Reservation Ha config error
```

- **show license summary**

  Affiche un résumé de l'état et de l'utilisation de la licence Smart.

  L'exemple suivant montre le résumé de l'ASA virtuel à l'aide d'une licence logicielle Smart standard :

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2016 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (ASAv-STD-1G)                     1 AUTHORIZED
```

  L'exemple suivant montre le résumé de l'ASA virtuel à l'aide de la réservation de licence permanente :

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: AUTHORIZED - RESERVED
```

- **show license usage**

  Affiche l'utilisation de la licence Smart.

  L'exemple suivant montre l'utilisation de l'ASA virtuel :

```
ciscoasa# show license usage

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
```

```
Status: AUTHORIZED
```

Affichage de l'UDI

Consultez la commande suivante pour afficher l'identifiant universel du produit (UDI) :

show license udi

L'exemple suivant montre l'UDI pour l'ASAv :

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

Débogage des licences logicielles Smart

Consultez les commandes suivantes pour le débogage de la mise en grappe :

- **debug license agent** {**error** | **trace** | **debug** | **all**}

  Active le débogage à partir de Smart Agent.

- **debug license** *level*

  Active différents niveaux de débogage de Smart Software Licensing Manager.

Communication avec Smart Software Manager

Cette section décrit comment votre périphérique communique avec Smart Software Manager.

Enregistrement de l'appareil et jetons

Pour chaque compte virtuel, vous pouvez créer un jeton d'enregistrement. Ce jeton est valide pendant 30 jours par défaut. Saisissez cet ID de jeton ainsi que les niveaux de droits lorsque vous déployez chaque périphérique ou lorsque vous enregistrez un périphérique existant. Vous pouvez créer un nouveau jeton si un jeton existant a expiré.

Remarque Châssis Firepower 4100/9300 : l'enregistrement du périphérique est configuré dans le châssis, et non sur le périphérique logique ASA.

Au démarrage après le déploiement, ou après avoir configuré manuellement ces paramètres sur un appareil existant, le périphérique s'enregistre auprès du Smart Software Manager. Lorsque le périphérique s'enregistre avec le jeton, le Smart Software Manager émet un certificat d'identification pour la communication entre le périphérique et le Smart Software Manager. Ce certificat est valide pendant 1 an, mais il sera renouvelé tous les 6 mois.

Communication périodique avec le Smart Software Manager

Le périphérique communique avec Smart Software Manager tous les 30 jours. Si vous apportez des modifications à Smart Software Manager, vous pouvez actualiser l'autorisation sur le périphérique pour que les modifications prennent effet immédiatement. Vous pouvez également attendre que le périphérique communique comme planifié.

Vous pouvez éventuellement configurer un mandataire HTTP.

ASA virtuel

L'ASA virtuel doit avoir un accès Internet directement ou par l'intermédiaire d'un mandataire HTTP au moins tous les 90 jours. La communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre périphérique restera conforme pendant 90 jours sans appel à Cisco. Après le délai de grâce, vous devez communiquer avec Smart Software Manager, sinon votre ASA virtuel ne sera pas conforme; l'opération n'est pas affectée par le reste.

Tous les autres modèles

L'ASA doit avoir un accès Internet directement ou par l'intermédiaire d'un mandataire HTTP au moins tous les 90 jours. La communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre périphérique fonctionnera jusqu'à 90 jours sans appel à Cisco. Après le délai de grâce, vous devez communiquer avec Smart Software Manager, sinon vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales, mais le fonctionnement n'en sera pas affecté autrement.

État de non-conformité

Le périphérique peut devenir non conforme dans les situations suivantes :

- Surutilisation : lorsque le périphérique utilise des licences non disponibles.
- Expiration de la licence : lorsqu'une licence à durée limitée expire.
- Absence de communication : lorsque le périphérique ne parvient pas à communiquer avec l'autorité de licence pour une nouvelle autorisation.

Pour vérifier si votre compte est dans un état de non-conformité ou s'en approche, vous devez comparer les droits actuellement utilisés par votre périphérique avec ceux de votre compte Smart.

Dans un état de non-conformité, le périphérique pourrait être limité, selon le modèle :

- ASA virtuel : l'ASA virtuel n'est pas affecté.
- Tous les autres modèles : tant que vous ne vous êtes pas enregistré auprès de l'autorité de licence, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales, mais le fonctionnement ne sera pas autrement affecté. Par exemple, les contextes existants au-dessus de la limite de licence Essentials peuvent continuer à s'exécuter et vous pouvez modifier leur configuration, mais vous ne pourrez pas ajouter un *nouveau* contexte. Si vous ne disposez pas de licences Essentials suffisantes lors de votre première inscription, vous ne pouvez pas configurer de fonctionnalités sous licence, y compris les fonctionnalités de cryptage renforcé.

Infrastructure Smart Call Home

Par défaut, un profil Smart Call Home existe dans la configuration qui spécifie l'URL de Smart Software Manager. Vous ne pouvez pas supprimer ce profil. Notez que la seule option configurable pour le profil de licence est l'URL d'adresse de destination de Smart Software Manager. Sauf indication contraire du TAC de Cisco, vous ne devez pas modifier l'URL de Smart Software Manager.



Remarque Pour le Châssis Firepower 4100/9300 , Smart Call Home pour les licences est configuré dans le superviseur Châssis Firepower 4100/9300 , et non sur l'ASA.

Vous ne pouvez pas désactiver Smart Call Home pour les licences logicielles Smart. Par exemple, même si vous désactivez Smart Call Home à l'aide de la commande **no service call-home**, la licence logicielle Smart n'est pas désactivée.

Les autres fonctions de Smart Call Home ne sont pas activées, sauf si vous les configurez expressément.

Gestion des certificats de licence Smart

L'ASA crée automatiquement un point de confiance contenant le certificat de la CA qui a émis le certificat de serveur Smart Transport ou Smart Call Home. Pour éviter une interruption du service si la hiérarchie d'émission du certificat de serveur change, configurez la commande **auto-update** zone pour activer la mise à jour automatique du groupe de certificats de confiance à des intervalles périodiques.

Le certificat de serveur reçu d'un serveur de journal système doit contenir « ServAuth » dans le champ Extended Key Usage (Utilisation de la clé étendue). Cette vérification sera effectuée uniquement pour les certificats non autosignés. Les certificats autosignés ne fournissent aucune valeur dans ce champ.

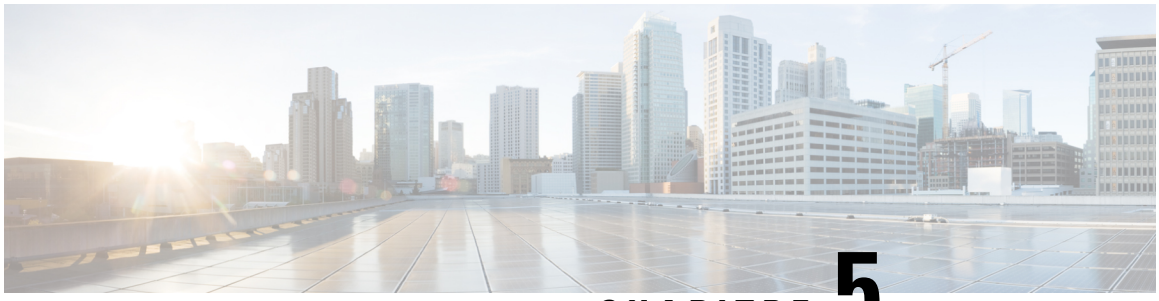
Historique des licences logicielles Smart

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de Secure Firewall 3100 pour la licence d'opérateur	9.18(1)	La licence d'opérateur permet l'inspection des protocoles Diameter, GTP/GPRS et SCTP. Commandes nouvelles ou modifiées : **feature carrier**
Réservation de licence permanente ASAv100	9.14(1.30)	L'ASAv100 prend désormais en charge la réservation de licence permanente à l'aide de l'ID de produit L-ASAV100SR-K9=. **Remarque :** tous les comptes ne sont pas approuvés pour la réservation de licence permanente.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge MSLA ASA virtuel	9.13(1)	L'ASA virtuel prend en charge le programme Contrat de licences de services gérés (MSLA) de Cisco, une structure d'octroi de licences et d'utilisation de logiciels conçue pour les clients et les partenaires de Cisco qui offrent des services gérés de logiciels à des tiers. MSLA est une nouvelle forme de licence Smart dans laquelle l'agent de licence Smart assure le suivi de l'utilisation des droits de licence par unités de temps. Commandes nouvelles ou modifiées : **license smart**, **mode**, **utility**, **custom-id**, **custom-info**, **privacy**, **transport type**, **transport url**, **transport proxy**
Licences flexibles ASA virtuel	9.13(1)	Les licences flexibles sont une nouvelle forme de licences Smart dans lesquelles n'importe quelle licence ASA virtuel peut désormais être utilisée sur n'importe quelle configuration de vCPU/mémoire ASA virtuel prise en charge. Les limites de session pour Secure Client (services client sécurisés) et le mandataire TLS seront déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée plutôt que par une limite de plateforme liée à un type de modèle. Commandes nouvelles ou modifiées : **show version**, **show vm**, **show cpu**, **show license features**
Modifications de licence pour les paires de basculement sur le Châssis Firepower 4100/9300	9.7(1)	Seule l'unité active demande les droits de licence. Auparavant, les deux unités demandaient des droits de licence. Pris en charge par FXOS 2.1.1.
Réservation de licence permanente pour l'amélioration des chaînes courtes d'ASA virtuel	9.6(2)	En raison d'une mise à jour de Smart Agent (vers 1.6.4), les codes de demande et d'autorisation utilisent désormais des chaînes plus courtes. Nous n'avons pas modifié de commandes.
Prise en charge du serveur satellite pour l'ASA virtuel	9.6(2)	Si vos périphériques ne peuvent pas accéder à Internet pour des raisons de sécurité, vous pouvez éventuellement installer un serveur satellite Smart Software Manager local en tant que machine virtuelle (VM). Nous n'avons pas modifié de commandes.
Réservation de licence permanente pour l'ASA sur le Châssis Firepower 4100/9300	9.6(2)	Pour les environnements hautement sécurisés où la communication avec Cisco Smart Software Manager n'est pas autorisée, vous pouvez demander une licence permanente pour l'ASA sur le Firepower 9300 et le Firepower 4100. Tous les droits de licence disponibles sont inclus dans la licence permanente, y compris les licences de niveau standard, de cryptage renforcé (le cas échéant), de contextes de sécurité et d'opérateur. FXOS 2.0.1 est nécessaire. Toute la configuration est effectuée sur le Châssis Firepower 4100/9300 ; aucune configuration n'est requise sur l'ASA.

Nom de la caractéristique	Versions de plateforme	Description
Réservation de licence permanente pour l'ASA virtuel	9.5(2.200) 9.6(2)	Pour les environnements hautement sécurisés où la communication avec Cisco Smart Software Manager n'est pas autorisée, vous pouvez demander une licence permanente pour l'ASA virtuel. Dans la version 9.6(2), nous avons également ajouté la prise en charge de cette fonctionnalité pour l'ASA virtuel sur Amazon Web Services. Cette fonctionnalité n'est pas prise en charge pour Microsoft Azure. Nous avons introduit les commandes suivantes : **license smart reservation, license smart reservation cancel, license smart reservation install, license smart reservation request universal, license smart reservation return**
Mise à niveau de Smart Agent vers la version 1.6	9.5(2.200) 9.6(2)	Smart Agent a été mis à niveau de la version 1.1 à la version 1.6. Cette mise à niveau prend en charge la réservation de licences permanentes et prend également en charge la définition du droit de licence de cryptage renforcé (3DES/AES) en fonction de l'autorisation définie dans votre compte de licence. **Remarque** Si vous rétrogradez à partir de la version 9.5(2.200), l'ASA virtuel ne conserve pas l'état d'enregistrement de la licence. Vous devez vous réenregistrer à l'aide de la commande **license smart register idtoken** *id_token* **force**; obtenir le jeton d'identification auprès de Smart Software Manager. Nous avons introduit les commandes suivantes : **show license status, show license summary, show license udi, show license usage** Nous avons modifié les commandes suivantes : **show license all, show tech-support license** Nous avons rendu obsolètes les commandes suivantes : **show license cert, show license entitlement, show license pool, show license registration**
Licence de cryptage renforcé (3DES) automatiquement appliquée pour l'ASA sur le Firepower 9300	9.5(2.1)	Pour les utilisateurs de Cisco Smart Software Manager standard, la licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement sur le châssis. Dans ce cas-là, aucune action supplémentaire n'est requise sur le Firepower 9300. **Remarque** Si vous utilisez le déploiement satellite du Smart Software Manager, pour utiliser ASDM et d'autres fonctionnalités de cryptage renforcé, après avoir déployé l'ASA, vous devez activer la licence de cryptage renforcé (3DES) à l'aide de l'interface de ligne de commande d'ASA. Cette fonctionnalité nécessite FXOS 1.1.3. Nous avons supprimé la commande suivante pour les configurations non satellites : **feature strong-encryption**

Nom de la caractéristique	Versions de plateforme	Description
Validation du certificat Smart Call Home/de licence Smart si la hiérarchie d'émission du certificat de serveur change	9.5(2)	La licence Smart utilise l'infrastructure Smart Call Home. Lorsque l'ASA configure pour la première fois les rapports anonymes de Smart Call Home en arrière-plan, il crée automatiquement un point de confiance contenant le certificat de la CA qui a émis le certificat de serveur Smart Call Home. L'ASA prend désormais en charge la validation du certificat si la hiérarchie d'émission du certificat de serveur change; vous pouvez activer la mise à jour automatique du groupe de confiance à des intervalles périodiques. Nous avons introduit la commande suivante : **auto-import**
Licence de transporteur	9.5(2)	La nouvelle licence de transporteur remplace la licence GTP/GPRS existante et comprend également la prise en charge de l'inspection SCTP et Diameter. Pour l'ASA sur le châssis Firepower 9300, la commande **feature mobile-sp** passera automatiquement à la commande **feature carrier**. Nous avons introduit ou modifié les commandes suivantes : **feature carrier, show activation-key, show license, show tech-support, show version**
Licences logicielles Cisco Smart pour l'ASA sur le Firepower 9300	9.4(1.150)	Nous avons introduit les licences logicielles Cisco Smart pour l'ASA sur le Firepower 9300 Nous avons introduit les commandes suivantes : **feature strong-encryption, feature mobile-sp, feature context**
Licence logicielle Smart de Cisco pour l'ASA virtuel	9.3(2)	Smart Software Licensing vous permet d'acheter et de gérer un ensemble de licences. Contrairement aux licences PAK, les licences Smart ne sont pas liées à un numéro de série ou à une clé de licence spécifique. Vous pouvez facilement déployer ou retirer des ASA virtuel sans avoir à gérer la clé de licence de chaque unité. Smart Software Licensing vous permet également de consulter votre utilisation et vos besoins en licences en un clin d'œil. Nous avons introduit les commandes suivantes : **clear configure license, debug license agent, feature tier, http-proxy, license smart, license smart deregister, license smart register, license smart renew, show license, show running-config license, throughput level**



CHAPITRE 5

Périphériques logiques pour le Firepower 4100/9300

Firepower 4100/9300 est une plateforme de sécurité flexible sur laquelle vous pouvez installer un ou plusieurs *périphériques logiques*. Ce chapitre décrit la configuration de l'interface de base et comment ajouter un périphérique logique autonome ou à haute accessibilité à l'aide de Firewall Chassis Manager. Pour ajouter un périphérique logique en grappe, consultez Grappe ASA pour le Firepower 4100/9300, à la page 445. Pour utiliser l'interface de ligne de commande de FXOS, consultez le guide de configuration de l'interface de ligne de commande FXOS. Pour des procédures FXOS et un dépannage plus avancés, consultez le guide de configuration FXOS.

- À propos des interfaces, à la page 175
- À propos des périphériques logiques, à la page 178
- Exigences et conditions préalables pour les combinaisons matérielles et logicielles , à la page 179
- Lignes directrices et limites relatives aux périphériques logiques, à la page 180
- Interfaces de configuration, à la page 181
- Configurer les périphériques logiques, à la page 186
- Historique des périphériques logiques, à la page 196

À propos des interfaces

Le Châssis Firepower 4100/9300 prend en charge les interfaces physiques et les interfaces EtherChannel (canal de port). Les interfaces EtherChannel peuvent comprendre jusqu'à 16 interfaces membres du même type.

Interface de gestion de châssis

L'interface de gestionnaire de châssis est utilisée pour la gestion du châssis FXOS par SSH ou Firewall Chassis Manager. Cette interface est distincte de l'interface de type gestion (mgmt) que vous affectez aux périphériques logiques pour la gestion des applications.

Pour configurer les paramètres de cette interface, vous devez les configurer à partir de l'interface de ligne de commande. Pour afficher des informations sur cette interface dans l'interface de ligne de commande FXOS, connectez-vous à la gestion locale et affichez le port de gestion :

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

Notez que l'interface de gestion du châssis reste active même si le câble physique ou le module SFP est débranché ou que la commande **mgmt-port shut** est exécutée ou si le périphérique logique est hors-ligne.

Remarque L'interface de gestion de châssis ne prend pas en charge les trames étendues.

Types d'interface

Les interfaces physiques et les interfaces EtherChannel (canal de port) peuvent être de l'un des types suivants :

- Données : à utiliser pour les données normales. Les interfaces de données ne peuvent pas être mises en commun entre les périphériques logiques, et les périphériques logiques ne peuvent pas communiquer avec d'autres périphériques logiques par le fond de panier Pour le trafic sur les interfaces de données, tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre périphérique logique.
- Data-sharing (partage de données) : à utiliser pour les données normales. Pris en charge uniquement avec les instances de conteneur, ces interfaces de données peuvent être partagées par un ou plusieurs dispositifs logiques/Instances de conteneur (Firewall Threat Defense-utilisant-Firewall Management Center seulement).
- Gestion : permet de gérer les instances d'application. Ces interfaces peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique. En fonction de votre application et de votre gestionnaire, vous pouvez ultérieurement activer la gestion à partir d'une interface de données; mais vous devez attribuer une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données.Pour en savoir plus sur l'interface de gestion de châssis distincte, consultez Interface de gestion de châssis, à la page 175.

Remarque La modification de l'interface de gestion entraînera le redémarrage du périphérique logique. Par exemple, une gestion des modifications de e1/1 à e1/2 entraînera le redémarrage du périphérique logique pour appliquer la nouvelle gestion.

- Créer un événement— Sert d'interface de gestion secondaire pour les périphériques Firewall Threat Defense-using- (en usage)Firewall Management Center.

Remarque Une interface Ethernet virtuelle est attribuée lors de l'installation de chaque instance applicative. Si l'application n'utilise pas d'interface événementielle, l'interface virtuelle sera dans un état "admin down".

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster (grappe) : à utiliser comme liaison de commande de grappe pour un périphérique logique en grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48. Le type de grappe est uniquement pris en charge sur les interfaces EtherChannel.

Reportez-vous à la table suivante pour la prise en charge des types d'interface pour les demandes Firewall Threat Defense et ASA dans les déploiements autonomes et en grappe.

Tableau 3 : Prise en charge des types d'interface

Application		Données	Données : sous-interface	Partage de données	Partage de données : sous-interface	Gestion	Créer des événements	Grappe (EtherChannel uniquement)	Grappe : sous-interface
Firewall Threat Defense	Instance native autonome	**Oui**	—	—	—	**Oui**	**Oui**	—	—
	Instance de conteneur autonome	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	—	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	—
	Instance de conteneur de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	**Oui**
ASA	Instance native autonome	**Oui**	—	—	—	**Oui**	—	**Oui**	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	—	**Oui**	—

Interfaces FXOS par rapport aux interfaces d'application

Le Firepower 4100/9300 gère les paramètres Ethernet de base des interfaces physiques et les interfaces EtherChannel (canal de port). Dans l'application, vous configurez les paramètres de niveau supérieur. Par

exemple, vous pouvez uniquement créer des EtherChannels dans FXOS; mais vous pouvez attribuer une adresse IP à l'EtherChannel dans l'application.

Les sections suivantes décrivent l'interaction entre FXOS et l'application pour les interfaces.

Sous-interfaces VLAN

Pour tous les périphériques logiques, vous pouvez créer des sous-interfaces VLAN dans l'application.

États indépendants de l'interface dans le châssis et dans l'application

Vous pouvez activer et désactiver administrativement les interfaces dans le châssis et dans l'application. Pour qu'une interface soit opérationnelle, elle doit être activée dans les deux systèmes d'exploitation. Étant donné que l'état de l'interface est contrôlé indépendamment, il se peut que vous ayez une incompatibilité entre le châssis et l'application.

À propos des périphériques logiques

Un périphérique logique vous permet d'exécuter une instance d'application (ASA ou Firewall Threat Defense) ainsi qu'une application de décochage facultative (Radware DefensePro) pour former une chaîne de services.

Lorsque vous ajoutez un périphérique logique, vous définissez également le type et la version de l'instance d'application, vous affectez des interfaces et vous configurez les paramètres de démarrage qui sont transmis à la configuration de l'application.



Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et Firewall Threat Defense) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

Périphériques logiques autonomes et en grappe

Vous pouvez ajouter les types d'unités logiques suivants :

- Autonome : un périphérique logique autonome fonctionne comme une unité autonome ou comme une unité dans une paire à haute disponibilité.
- Grappe : un appareil logique en grappe vous permet de regrouper plusieurs unités ensemble, offrant toute la commodité d'un seul appareil (gestion, intégration dans un réseau) tout en obtenant le débit accru et la redondance de plusieurs périphériques. Les périphériques à modules multiples, comme le périphérique Firepower 9300, prennent en charge la mise en grappe à l'intérieur des châssis. Pour le périphérique Firepower 9300, les trois modules doivent faire partie de la grappe, à la fois pour les instances natives et de conteneur.

Exigences et conditions préalables pour les combinaisons matérielles et logicielles

Le Firepower 4100/9300 prend en charge plusieurs modèles, modules de sécurité, types d'applications, et de haute disponibilité et d'évolutivité. Consultez les exigences suivantes pour connaître les combinaisons autorisées.

Exigences du périphérique Firepower 9300

L'appareil Firepower 9300 comprend 3 logements pour module de sécurité et plusieurs types de modules de sécurité. Consultez les exigences suivantes :

- Security Module Types (types de modules de sécurité) : Vous pouvez installer des modules de différents types dans le périphérique Firepower 9300. Par exemple, vous pouvez installer le SM-48 comme module 1, le SM-40 comme module 2 et le SM-56 comme module 3.
- Instances natives et de conteneur : lorsque vous installez une instance de conteneur sur un module de sécurité, ce module ne peut prendre en charge que d'autres instances de conteneur. Une instance native utilise toutes les ressources d'un module, vous ne pouvez donc installer qu'une seule instance native sur un module. Vous pouvez utiliser des instances natives sur certains modules et des instances de conteneur sur les autres modules. Par exemple, vous pouvez installer une instance native sur le module 1 et le module 2, mais des instances de conteneur sur le module 3.
- Mise en grappe : tous les modules de sécurité de la grappe, qu'elle soit intra-châssis ou inter-châssis, doivent être du même type. Vous pouvez avoir différentes quantités de modules de sécurité installés dans chaque châssis, bien que tous les modules présents dans le châssis doivent appartenir à la grappe, y compris les logements vides. Par exemple, vous pouvez installer 2 SM-40 dans le châssis 1 et 3 SM-40 dans le châssis 2. Vous ne pouvez pas utiliser la mise en grappe si vous installez 1 SM-48 et 2 SM-40 dans le même châssis.
- High Availability (haute disponibilité) : la haute disponibilité est prise en charge uniquement entre les modules de même type sur le périphérique Firepower 9300. Cependant, les deux châssis peuvent comprendre des modules mixtes. Par exemple, chaque châssis a un SM-40, SM-48 et SM-56. Vous pouvez créer des paires à haute disponibilité entre les modules SM-40, entre les modules SM-48 et entre les modules SM-56.
- Types d'applications ASA et Firewall Threat Defense :Vous pouvez installer différents types d'applications sur des modules distincts dans le châssis. Par exemple, vous pouvez installer ASA sur le module 1 et le module 2, et Firewall Threat Defense sur le module 3.
- Versions ASA ou Firewall Threat Defense : vous pouvez exécuter différentes versions d'un type d'instance d'application sur des modules distincts ou en tant qu'instances de conteneur distinctes sur le même module. Par exemple, vous pouvez installer Firewall Threat Defense 6.3 sur le module 1, Firewall Threat Defense 6.4 sur le module 2 et Firewall Threat Defense 6.5 sur le module 3.

Exigences du périphérique Firepower 4100

L'appareil Firepower 4100 est offert en plusieurs modèles. Consultez les exigences suivantes :

- Instances natives et de conteneur : lorsque vous installez une instance de conteneur sur une Firepower 4100, cet appareil ne peut prendre en charge que d'autres instances de conteneur. Une instance native

utilise toutes les ressources d'un périphérique, vous ne pouvez donc installer qu'une seule instance native sur le périphérique.

- Mise en grappe : tous les châssis de la grappe doivent être du même modèle.
- Haute disponibilité : la haute disponibilité est uniquement prise en charge entre les modèles du même type.
- Types d'application ASA et Firewall Threat Defense : Firepower 4100 ne peut exécuter qu'un seul type d'application.

Lignes directrices et limites relatives aux périphériques logiques

Consultez les sections suivantes pour connaître les instructions et les limites.

Lignes directrices et limites des interfaces

Adresses MAC par défaut

Les attributions d'adresses MAC par défaut dépendent du type d'interface.

- Interfaces physiques : l'interface physique utilise l'adresse MAC gravée.
- EtherChannels : Pour un EtherChannel, toutes les interfaces du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels. L'interface du canal de port utilise une adresse MAC unique provenant d'un pool; L'appartenance à l'interface n'affecte pas l'adresse MAC.

Lignes directrices et limites générales

Mode pare-feu

Vous pouvez définir le mode de pare-feu routé ou transparent dans la configuration de démarrage des Firewall Threat Defense et ASA.

Haute disponibilité

- Configurez la haute disponibilité dans la configuration de l'application.
- Vous pouvez utiliser n'importe quelle interface de données comme liens de basculement et d'état.Les interfaces de partage de données ne sont pas prises en charge.

Mode contexte

- Activez le mode de contexte multiple dans l'ASA après le déploiement.

Exigences et prérequis pour la haute accessibilité

- Les deux unités d'une configuration de basculement à haute accessibilité doivent :
  - Être sur un châssis séparé; la haute accessibilité intra-châssis pour le Firepower 9300 n'est pas prise en charge.
  - être du même modèle.
  - Avoir les mêmes interfaces que celles des périphériques logiques à haute accessibilité.
  - Avoir le même nombre et les mêmes types d'interfaces. Toutes les interfaces doivent être préconfigurées de manière identique dans FXOS avant que vous activiez la haute accessibilité.
- La haute accessibilité est uniquement prise en charge entre les modules de même type sur le Firepower 9300; toutefois, les deux châssis peuvent inclure des modules mixtes. Par exemple, chaque châssis a un SM-56, SM-48 et SM-40. Vous pouvez créer des paires à haute accessibilité entre les modules SM-56, entre les modules SM-48 et entre les modules SM-40.
- Pour les autres exigences du système en matière de haute accessibilité, consultez Configuration système requise pour Failover (basculement), à la page 274.

Interfaces de configuration

Par défaut, les interfaces physiques sont désactivées. Vous pouvez activer les interfaces, ajouter des canaux EtherChannels, et modifier les propriétés de l'interface et .

Remarque Si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation ASA.

Configurer une interface physique

Vous pouvez physiquement activer et désactiver les interfaces, ainsi que définir la vitesse d'interface et le mode duplex. Pour utiliser une interface, elle doit être physiquement activée dans FXOS et logiquement activée dans l'application.

Remarque

- Dans le cas de QSFPH40G-CUxM, la négociation automatique est toujours activée par défaut et vous ne pouvez pas la désactiver.
- Si vous remplacez un module SFP sur un port par un module SFP différent, la vitesse, les conditions de duplex et la négociation automatique de l'interface ne sont pas mises à jour automatiquement. Vous devez reconfigurer manuellement l'interface.

Avant de commencer

- Les interfaces qui sont déjà membres d'un EtherChannel ne peuvent pas être modifiées individuellement. Assurez-vous de configurer les paramètres avant de les ajouter au canal EtherChannel.

Procédure

Étape 1 Entrez le mode d'interface.

scope eth-uplink

scope fabric a

Étape 2 Activez l'interface.

enter interface *identifiant_de_l_interface*

enable

Exemple :

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

Remarque
Les interfaces qui sont déjà membres d'un canal de port ne peuvent pas être modifiées individuellement. Si vous utilisez la commande **enter interface** ou **scope interface** sur une interface membre d'un canal de port, vous recevrez un message d'erreur indiquant que l'objet n'existe pas. Vous devez modifier les interfaces à l'aide de la commande **enter interface** avant de les ajouter à un canal de port.

Étape 3 (Facultatif) Définir le délai anti-rebond.

set debounce-time 5000 {Enter a value between 0-15000 milli-seconds}

Exemple :

```
Firepower /eth-uplink/fabric/interface # set debounce-time 5000
```

Exemple :

Remarque
La configuration du délai antirebond n'est pas prise en charge sur les interfaces 1G.

Étape 4 (Facultatif) Définissez le type d'interface.

set port-type {**data** | **mgmt** | **cluster**}

Exemple :

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

Le mot clé **data** est le type par défaut. Ne choisissez pas le mot clé **cluster**; par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48.

Étape 5 Activez ou désactivez la négociation automatique, si elle est prise en charge pour votre interface.

set auto-negotiation {**on** | **off**}

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

Étape 6 Définissez la vitesse de l'interface.

set admin-speed {**1gbps** | **10gbps** | **40gbps** | **100gbps**}

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

Étape 7 Définissez le mode duplex de l'interface.

set admin-duplex {**fullduplex** | **halfduplex**}

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

Étape 8 Si vous avez modifié la politique de contrôle de flux par défaut, elle est déjà appliquée aux interfaces. Si vous avez créé une nouvelle politique, appliquez-la à l'interface.

set flow-control-policy *name*

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

Étape 9 Enregistrez la configuration.

commit-buffer

Exemple :

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

Ajouter un canal EtherChannel (canal de port)

Un EtherChannel (également appelé canal de port) peut inclure jusqu'à 16 interfaces membres de même type de support et de capacité, et doit être réglé à la même vitesse et au même duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité. Le protocole LACP (Link Aggregation Control Protocol) agrège les interfaces en échangeant les LACPDU (Link Aggregation Control Protocol Data Unit) entre deux périphériques réseau.

Vous pouvez configurer chaque interface physique de données dans un EtherChannel pour qu'elle soit :

- Actif : envoie et reçoit les mises à jour du protocole LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.
- Activé : l'EtherChannel est toujours activé et le protocole LACP n'est pas utilisé. Un EtherChannel « activé » ne peut établir une connexion qu'avec un autre EtherChannel « activé ».



Remarque Cela peut prendre jusqu'à trois minutes à un EtherChannel de revenir à l'état opérationnel si vous faites passer son mode de On (Activé) à Actif ou de Actif à Activé.

Les interfaces sans données ne prennent en charge que le mode actif.

Le protocole LACP coordonne l'ajout et la suppression automatiques des liens vers l'EtherChannel sans l'intervention de l'utilisateur. Il gère également les erreurs de configuration et vérifie que les deux extrémités des interfaces membres sont connectées au groupe de canaux approprié. Le mode « Activé» ne peut pas utiliser les interfaces en veille dans le groupe de canaux lorsqu'une interface tombe en panne et que la connectivité et les configurations ne sont pas vérifiées.

Lorsque Châssis Firepower 4100/9300 crée un EtherChannel, l'EtherChannel reste dans un état **Suspendu** pour le mode LACP actif ou à l'arrêt pour le mode LACP **activé** jusqu'à ce que vous l'affectiez à un périphérique logique, même si le lien physique est actif. L'EtherChannel sortira de l'état **Suspendu** dans les situations suivantes :

- L'EtherChannel est ajouté en tant qu'interface de données ou de gestion pour un périphérique logique autonome
- L'EtherChannel est ajouté en tant qu'interface de gestion ou liaison de commande de grappe pour un périphérique logique qui fait partie d'une grappe
- L'EtherChannel est ajouté en tant qu'interface de données pour un périphérique logique qui fait partie d'une grappe et au moins une unité a rejoint la grappe

Notez que l'EtherChannel ne s'affiche pas tant que vous ne l'avez pas affecté à un périphérique logique. Si l'EtherChannel est retiré de l'unité logique ou si l'unité logique est supprimée, il repasse à l'état **Suspendu** ou **Inactif**.

Procédure

Étape 1 Entrez le mode d'interface.

scope eth-uplink

scope fabric a

Étape 2 Créez le canal de port :

create port-channel *id*

enable

Étape 3 Affectez des interfaces membres :

create member-port *interface_id*

Vous pouvez ajouter jusqu'à 16 interfaces du même type et de la même vitesse. Les interfaces membres doivent être réglées à la même vitesse et au même duplex et doivent correspondre à la vitesse et au duplex que vous avez configurés pour ce canal de port. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité.

Exemple :

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

Étape 4 (Facultatif) Définissez le type d'interface.

set port-type {**data** | **mgmt** | **cluster**}

Exemple :

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

Le mot clé **data** est le type par défaut. Ne choisissez pas le mot clé **cluster**, sauf si vous souhaitez utiliser ce canal de port comme liaison de commande de grappe au lieu de la valeur par défaut.

Étape 5 Définissez la vitesse d'interface requise pour les membres du canal de port.

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

Si vous ajoutez une interface membre qui n'a pas la vitesse spécifiée, elle ne pourra pas rejoindre le canal de port. La valeur par défaut est **10gbps**.

Exemple :

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

Étape 6 (Facultatif) Définissez le duplex requis pour les membres du canal de port.

set duplex {**fullduplex** | **halfduplex**}

Si vous ajoutez une interface membre configurée avec le duplex précisé, elle ne rejoindra pas le canal de port. La valeur par défaut est **fullduplex**.

Exemple :

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

Étape 7 Activez ou désactivez la négociation automatique, si elle est prise en charge pour votre interface.

set auto-negotiation {**on** | **off**}

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

Étape 8 Définissez le mode du canal de port LACP pour les interfaces de données.

Pour les interfaces sans données, le mode est toujours actif.

set port-channel-mode {**active** | **on**}

Exemple :

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

Étape 9 Si vous avez modifié la politique de contrôle de flux par défaut, elle est déjà appliquée aux interfaces. Si vous avez créé une nouvelle politique, appliquez-la à l'interface.

set flow-control-policy *name*

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

Étape 10 Validez la configuration :

commit-buffer

Configurer les périphériques logiques

Ajoutez un périphérique logique autonome ou une paire à haute disponibilité sur le Châssis Firepower 4100/9300 .

Pour la mise en grappe, consultez #unique_219.

Ajouter un ASA autonome

Les périphériques logiques autonomes fonctionnent seuls ou dans une paire haute disponibilité. Sur Firepower 9300 avec plusieurs modules de sécurité, vous pouvez déployer une grappe ou des appareils autonomes. La grappe doit utiliser tous les modules. Par conséquent, vous ne pouvez pas combiner une grappe à deux modules et un seul périphérique autonome.

Vous pouvez déployer un ASA routé ou transparent en mode pare-feu à partir de Châssis Firepower 4100/9300 .

Pour le mode à contextes multiples, vous devez d'abord déployer le périphérique logique, puis activer le mode à contextes multiples dans l'application ASA.

Avant de commencer

- Téléchargez l'image de l'application que vous souhaitez utiliser pour le périphérique logique à partir de Cisco.com), puis téléchargez cette image sur Châssis Firepower 4100/9300 .

Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et Firewall Threat Defense) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

- Configurez une interface de gestion à utiliser avec le périphérique logique. L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que le port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (dans FXOS, vous pouvez la voir s'afficher comme MGMT, management0 ou autres noms semblables)
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce périphérique
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - Adresse IP de la passerelle

Procédure

Étape 1 Entrez le mode de services de sécurité.

scope ssa

Exemple :

```
Firepower# scope ssa
Firepower /ssa #
```

Étape 2 Définissez la version de l'image de l'instance de l'application.

a) Affichez les images disponibles. Notez le numéro de version que vous souhaitez utiliser.

show app

Exemple :

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) Définissez la portée au niveau du module de sécurité/logement du moteur.

scope slot *slot_id*

L'id *slot_id* est toujours 3 pour la Firepower 4100 et 1, 2 ou 3 pour la Firepower 9300.

Exemple :

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) Créez l'instance d'application.

enter app-instance asa *device_name*

Device_name peut comporter entre 1 et 64 caractères. Vous utiliserez ce nom de périphérique lorsque vous créerez le périphérique logique pour cette instance.

Exemple :

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

d) Définissez la version de l'image ASA.

set startup-version *version*

Exemple :

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) Quittez pour passer en mode logement.

exit

Exemple :

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) Quittez le mode ssa.

exit

Exemple :

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Exemple :

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Étape 3 Créez le périphérique logique.

enter logical-device *device_name* **asa** *slot_id* **standalone**

Utilisez le même *Device_name* que celui de l'instance d'application que vous avez ajoutée précédemment.

Exemple :

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

Étape 4 Attribuez les interfaces de gestion et de données au périphérique logique. Répétez l'opération pour chaque interface.

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name* : le nom est utilisé par le superviseur Châssis Firepower 4100/9300 . il ne s'agit pas du nom d'interface utilisé dans la configuration de l'ASA.
- *description* : utilisez des guillemets (") autour des expressions avec des espaces.

L'interface de gestion n'est pas la même que le port de gestion du châssis. Vous activerez et configurerez ultérieurement ces interfaces dans l'ASA, y compris la définition des adresses IP.

Exemple :

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

Étape 5 Configurez les renseignements de démarrage de gestion.

a) Créez l'objet de démarrage.

create mgmt-bootstrap asa

Exemple :

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) Spécifiez le mode de pare-feu, routage ou transparent.

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

En mode routage, l'appareil est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) Spécifiez le mot de passe d'administrateur et d'activation.

create bootstrap-key-secret PASSWORD

set value

Saisissez une valeur *mot de passe*

Confirmez la valeur : *mot de passe*

exit

Exemple :

L'utilisateur admin ASA et le mot de passe d'activation préconfigurés sont utiles pour la récupération du mot de passe. si vous avez un accès FXOS, vous pouvez réinitialiser le mot de passe de l'utilisateur admin en cas d'oubli.

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) Configurez les paramètres de l'interface de gestion IPv4.

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) Configurez les paramètres de l'interface de gestion IPv6.

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) Quittez le mode de démarrage de gestion.

exit

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Étape 6 Enregistrez la configuration.

commit-buffer

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Vérifiez l'état du déploiement à l'aide de la commande **show app-instance**. L'instance d'application est en cours d'exécution et prête à être utilisée lorsque l'état **Admin State** est **Enabled** (Activé) et que l'état **Oper State** est **Online** (En ligne).

Exemple :

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- ------------
asa        asa1       2          Disabled    Not Installed                    9.12.1
    Native                   Not Applicable  None
ftd        ftd1       1          Enabled     Online           6.4.0.49        6.4.0.49
    Container   Default-Small Not Applicable  None
```

Étape 7 Consultez le guide de configuration ASA pour commencer à configurer votre politique de sécurité.

Exemple

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

Ajouter une paire à haute disponibilité

La haute disponibilité Firewall Threat DefenseASA (également appelée basculement) est configurée dans l'application, pas dans FXOS. Toutefois, pour préparer votre châssis à la haute disponibilité, consultez les étapes suivantes.

Avant de commencer

Consultez la section Configuration système requise pour Failover (basculement), à la page 274.

Procédure

Étape 1 Attribuez les mêmes interfaces à chaque périphérique logique.

Étape 2 Attribuez une ou deux interfaces de données au basculement et à l'état des liens.

Ces interfaces échangent le trafic à haute disponibilité entre les deux châssis. Nous vous recommandons d'utiliser une interface de données de 10 Go pour un basculement et une liaison d'état combinés. Si vous avez des interfaces disponibles, vous pouvez utiliser des liaisons de basculement et d'état distincts; le lien d'état nécessite le plus de bande passante. Vous ne pouvez pas utiliser l'interface de type de gestion pour la liaison

de basculement ou d'état. Nous vous recommandons d'utiliser un commutateur entre les châssis, afin qu'aucun autre périphérique ne se trouve sur le même segment de réseau que les interfaces de basculement.

Étape 3 Activez la haute disponibilité sur les périphériques logiques. Consultez Basculement pour la haute disponibilité, à la page 273.

Étape 4 Si vous modifiez les interfaces après avoir activé la haute disponibilité, modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

Remarque
Dans le cas de l'ASA, si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation de l'ASA.

Modifier une interface sur un périphérique logique ASA

Vous pouvez allouer, annuler l'allocation ou remplacer une interface de gestion sur un périphérique logique ASA. ASDM détecte automatiquement les nouvelles interfaces.

L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration de l'ASA. Cependant, si vous supprimez une interface allouée dans FXOS (par exemple, si vous supprimez un module de réseau, supprimez un EtherChannel ou réaffectez une interface allouée à un EtherChannel) et que l'interface est utilisée dans votre politique de sécurité, la suppression aura une incidence sur la configuration de l'ASA. Dans ce cas, la configuration de l'ASA conserve les commandes d'origine afin que vous puissiez apporter les ajustements nécessaires. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation de l'ASA.



Remarque Vous pouvez modifier les membres d'un EtherChannel alloué sans affecter le périphérique logique.

Avant de commencer

- Configurez vos interfaces et ajoutez tous les EtherChannels en fonction de Configurer une interface physique, à la page 181 et Ajouter un canal EtherChannel (canal de port), à la page 183.
- Si vous souhaitez ajouter une interface déjà allouée à un EtherChannel (par exemple, toutes les interfaces sont allouées par défaut à une grappe), vous devez d'abord désallouer l'interface du périphérique logique, puis ajouter l'interface à l'EtherChannel. Pour un nouvel EtherChannel, vous pouvez ensuite l'affecter au périphérique.
- Pour la mise en grappe ou le basculement, assurez-vous d'ajouter ou de supprimer l'interface sur toutes les unités. Nous vous recommandons d'effectuer les modifications d'interface d'abord sur l'unité de données ou de secours, puis sur l'unité de contrôle ou l'unité active. Les nouvelles interfaces sont ajoutées dans un état administrativement inactif, de sorte qu'elles n'affectent pas la supervision des interfaces.

Procédure

Étape 1 Entrez le mode de services de sécurité :

Firepower# **scope ssa**

Étape 2 Modifiez le périphérique logique :

Firepower /ssa # **scope logical-device** *device_name*

Étape 3 Annulez l'allocation d'une interface du périphérique logique :

Firepower /ssa/logical-device # **delete external-port-link** *name*

Saisissez la commande **show external-port-link** pour afficher les noms d'interface.

Pour une interface de gestion, supprimez l'interface actuelle, puis validez votre modification à l'aide de la commande **commit-buffer** avant d'ajouter la nouvelle interface de gestion.

Étape 4 Attribuez une nouvelle interface à l'unité logique :

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

Étape 5 Validez la configuration :

commit-buffer

Validez la transaction dans la configuration système.

Se connecter à la console de l'application

Suivez la procédure ci-dessous pour vous connecter à la console de l'application.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module *slot_number* {**console** | **telnet**}

Pour vous connecter au moteur de sécurité d'un périphérique qui ne prend pas en charge plusieurs modules de sécurité, utilisez toujours **1** comme *slot_number*.

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
```

```
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Étape 2 Connectez-vous à la console d'application.

connect asa *name*

Pour afficher les noms des instances, entrez la commande sans nom.

Exemple :

```
Firepower-module1> connect asa asa1
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

Étape 3 Quittez la console d'application pour accéder à l'interface de ligne de commande du module FXOS.

- ASA : Saisissez **Ctrl-a, d**

Étape 4 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Exemple

Dans l'exemple suivant, une connexion est établie à un ASA sur le module de sécurité 1, puis retourne au niveau de superviseur du Interface de ligne de commande FXOS.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

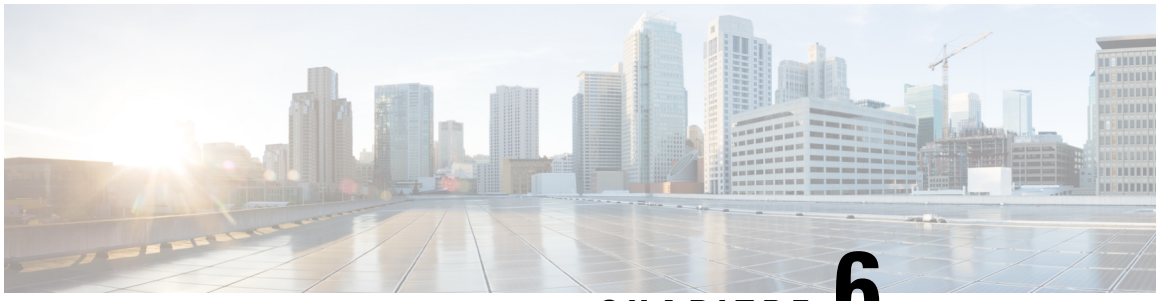
Firepower-module1>connect asa asa1
asa> ~
telnet> quit
```

```
Connection closed.
Firepower#
```

Historique des périphériques logiques

Fonctionnalités	Version	Détails
ASA pour le Firepower 4112	9.14(1)	Nous avons lancé le Firepower 4112. **Remarque** FXOS 2.8.1 est nécessaire.
Prise en charge du Firepower 9300 SM-56	9.12.2	Nous avons lancé le module de sécurité SM-56. **Remarque** FXOS 2.6.1.157 est nécessaire.
ASA pour les Firepower 4115, 4125 et 4145	9.12(1)	Nous avons lancé les Firepower 4115, 4125 et 4145. **Remarque** FXOS 2.6.1 est nécessaire.
Prise en charge des Firepower 9300 SM-40 et SM-48	9.12.1	Nous avons lancé les modules de sécurité SM-40 et SM-48. **Remarque** FXOS 2.6.1 est nécessaire.
Prise en charge d'ASA et de Firewall Threat Defense sur des modules distincts du même Firepower 9300	9.12.1	Vous pouvez maintenant déployer ASA et des périphériques logiques Firewall Threat Defense sur le même Firepower 9300. **Remarque** FXOS 2.6.1 est nécessaire.
Adresse IP personnalisable par liaison de commande de grappe pour le Firepower 4100/9300	9.10.1	Par défaut, la liaison de commande de grappe utilise le réseau 127.2.0.0/16. Vous pouvez maintenant définir le réseau lorsque vous déployez la grappe dans FXOS. Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot_id*. Cependant, certains déploiements réseau ne permettent pas le passage du trafic 127.2.0.0/16. Par conséquent, vous pouvez maintenant définir un sous-réseau personnalisé /16 pour la liaison de commande de grappe dans FXOS, à l'exception des adresses de boucle avec retour (127.0.0.0/8) et de multidiffusion (224.0.0.0/4). **Remarque** FXOS 2.4.1 est nécessaire. Commandes FXOS nouvelles ou modifiées : **set cluster-control-link network**

Fonctionnalités	Version	Détails
Prise en charge des données EtherChannels en mode activé	9.10.1	Vous pouvez maintenant définir les données et les EtherChannels de partage de données en mode LACP actif ou en mode Activé. Les autres types d'EtherChannels ne prennent en charge que le mode actif. **Remarque** FXOS 2.4.1 est nécessaire. Commandes FXOS nouvelles ou modifiées : **set port-channel-mode**
Amélioration de la mise en grappe inter-sites pour l'ASA sur le Châssis Firepower 4100/9300	9.7(1)	Vous pouvez maintenant configurer l'ID de site pour chaque Châssis Firepower 4100/9300 lorsque vous déployez la grappe ASA. Auparavant, vous deviez configurer l'ID de site dans l'application ASA; cette nouvelle fonctionnalité facilite le déploiement initial. Notez que vous ne pouvez plus définir l'ID de site dans la configuration ASA. En outre, pour une meilleure compatibilité avec la mise en grappe inter-sites, nous vous recommandons de mettre à niveau vers ASA 9.7(1) et FXOS 2.1.1, ce qui comprend plusieurs améliorations de la stabilité et des performances. Nous avons modifié la commande suivante : **site-id**
Prise en charge de Firepower 4100	9.6(1)	Avec FXOS 1.1.4, l'ASA prend en charge la mise en grappe inter-châssis sur le Firepower 4100. Nous n'avons pas modifié de commandes.
Mise en grappe inter-châssis pour 6 modules et mise en grappe inter-sites pour l'application ASA Firepower 9300	9.5(2.1)	Grâce à FXOS 1.1.3, vous pouvez désormais activer la mise en grappe inter-châssis et par extension inter-sites. Vous pouvez inclure jusqu'à 6 modules dans un maximum de 6 châssis. Nous n'avons pas modifié de commandes.
Mise en grappe d'ASA intra-châssis pour le Firepower 9300	9.4(1.150)	Vous pouvez mettre en grappe jusqu'à 3 modules de sécurité dans le châssis Firepower 9300. Tous les modules dans le châssis doivent appartenir à la grappe. Nous avons introduit les commandes suivantes : **cluster replication delay, debug service-module, management-only individual, show cluster chassis**



CHAPITRE 6

Mode pare-feu transparent ou routé

Ce chapitre décrit comment définir le mode du pare-feu routé ou transparent, ainsi que le fonctionnement du pare-feu dans chaque mode de pare-feu.

Vous pouvez définir le mode de pare-feu indépendamment pour chaque contexte en mode de contexte multiple.

- À propos du mode pare-feu, à la page 199
- Paramètres d'usine, à la page 208
- Lignes directrices sur le mode pare-feu, à la page 208
- Définir le mode du pare-feu, à la page 210
- Exemples de mode de pare-feu, à la page 211
- Historique du mode de pare-feu, à la page 221

À propos du mode pare-feu

Le ASA prend en charge deux modes de pare-feu : le mode de pare-feu routé et le mode de pare-feu transparent.

À propos du mode de pare-feu routé

En mode routage, l'ASA est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Vous pouvez partager des interfaces de couche 3 entre les contextes.

Avec le routage et le pont intégrés, vous pouvez utiliser un « groupe de ponts » dans lequel vous regroupez plusieurs interfaces sur un réseau, et l'ASA utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. Les routes ASA entre les BVI et les interfaces de routage normales. Si vous n'avez pas besoin du mode à contextes multiples ou de mise en grappe, ni d'interfaces membre EtherChannel ou VNI, vous pouvez envisager d'utiliser le mode routé au lieu du mode transparent. En mode routé, vous pouvez avoir un ou plusieurs groupes de ponts isolés comme en mode transparent, mais vous pouvez également avoir des interfaces de routage normales pour un déploiement mixte.

À propos du mode de pare-feu transparent

Classiquement, un pare-feu est un saut routé et agit comme une passerelle par défaut pour les hôtes qui se connectent à l'un de ses sous-réseaux filtrés. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré

comme un saut de routeur vers les appareils connectés. Cependant, comme tout autre pare-feu, le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications normales de pare-feu sont en place.

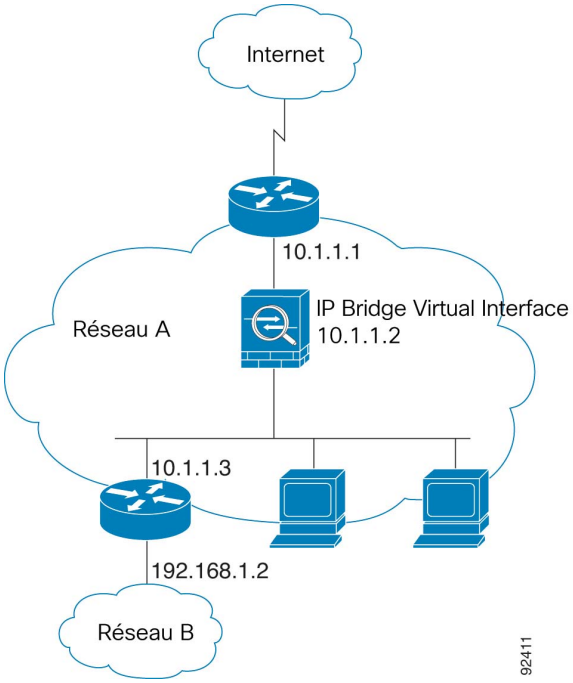
La connectivité de couche 2 est obtenue à l'aide d'un « groupe de ponts » où vous regroupez les interfaces interne et externe d'un réseau, où l'ASA utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. Vous pouvez avoir plusieurs groupes de ponts pour plusieurs réseaux. En mode transparent, ces groupes de ponts ne peuvent pas communiquer entre eux.

Utilisation du pare-feu transparent au sein de votre réseau

L'ASA relie le même réseau entre ses interfaces. Étant donné que le pare-feu n'est pas un tronçon de routage, vous pouvez facilement introduire un pare-feu transparent dans un réseau existant.

La figure suivante montre un réseau de pare-feu transparent typique où les périphériques externes se trouvent sur le même sous-réseau que les périphériques internes. Le routeur interne et les hôtes semblent être directement connectés au routeur externe.

Illustration 22 : Réseau de pare-feu transparent



Interface Management (gestion)

En plus de chaque adresse IP d'interface virtuelle de pont (BVI), vous pouvez ajouter une interface de Management (gestion) *logement*/*port* distincte qui ne fait partie d'aucun groupe de ponts et qui autorise uniquement le trafic de gestion vers l'ASA. Pour obtenir plus de renseignements, consultez Interface de gestion, à la page 672.

Trafic de transfert pour les fonctionnalités en mode routé

Pour les fonctionnalités qui ne sont pas directement prises en charge sur le pare-feu transparent, vous pouvez laisser le trafic passer pour que les routeurs en amont et en aval prennent en charge la fonctionnalité. Par

exemple, en utilisant une règle d'accès, vous pouvez autoriser le trafic DHCP (au lieu de la fonction de relais DHCP non prise en charge) ou le trafic de multidiffusion comme celui créé par IP/TV. Vous pouvez également établir des contiguïtés de protocole de routage par l'intermédiaire d'un pare-feu transparent; vous pouvez autoriser le trafic OSPF, RIP, EIGRP ou BGP en fonction d'une règle d'accès. De même, des protocoles comme HSRP ou VRRP peuvent passer par le ASA.

À propos des groupes de ponts

Un groupe de ponts est un groupe d'interfaces que ASA relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Comme toute autre interface de pare-feu, le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications normales de pare-feu sont en place.

Interface BVI (Bridge Virtual Interface)

Chaque groupe de ponts comprend une interface virtuelle de pont (BVI). ASA utilise l'adresse IP des BVI comme adresse source pour les paquets provenant du groupe de ponts. L'adresse IP BVI doit se trouver sur le même sous-réseau que les interfaces membres du groupe de ponts. Les BVI ne prennent pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.

En mode transparent : seules les interfaces des membres du groupe de ponts sont nommées et peuvent être utilisées avec les fonctionnalités basées sur l'interface.

En mode routé : les BVI servent de passerelle entre le groupe de ponts et les autres interfaces routées. Pour le routage entre groupes de ponts/interfaces routées, vous devez nommer le BVI. Pour certaines fonctionnalités basées sur l'interface, vous pouvez utiliser le BVI lui-même :

- Access Rules (règles d'accès) : vous pouvez configurer des règles d'accès pour les interfaces des membres des groupes de ponts et pour les BVI; pour les règles de trafic entrant, l'interface membre est vérifiée en premier. Pour les règles de trafic sortant, les BVI sont vérifiés en premier.
- Serveur DHCPv4 : seuls les BVI prennent en charge la configuration de serveur DHCPv4.
- Routes statiques : vous pouvez configurer des routes statiques pour les BVI; vous ne pouvez pas configurer de routage statique pour les interfaces membres.
- Serveur syslog et autre trafic provenant de ASA : lorsque vous spécifiez un serveur syslog (ou un serveur SNMP, ou un autre service où le trafic provient de ASA), vous pouvez spécifier une interface BVI ou une interface membre.

Si vous ne nommez pas les BVI en mode routé, ASA n'acheminera pas le trafic du groupe de ponts. Cette configuration reproduit le mode de pare-feu transparent pour le groupe de ponts. Si vous n'avez pas besoin du mode à contextes multiples ni de mise en grappe, ni d'interfaces membre EtherChannel ou VNI, vous pouvez envisager d'utiliser le mode routé à la place. En mode routé, vous pouvez avoir un ou plusieurs groupes de ponts isolés comme en mode transparent, mais vous pouvez également avoir des interfaces de routage normales pour un déploiement mixte.

Groupes de ponts en mode pare-feu transparent

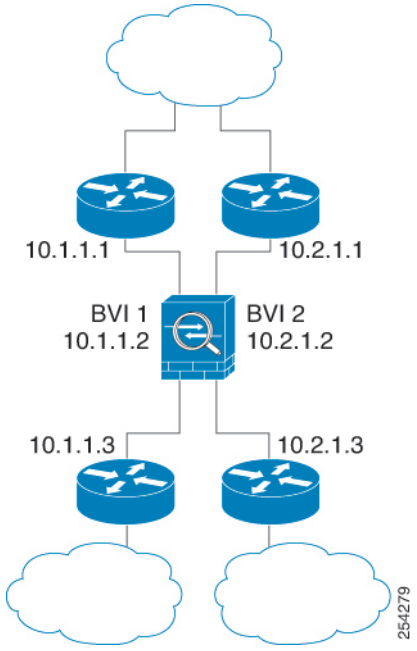
Le trafic des groupes de ponts est isolé des autres groupes de ponts; le trafic n'est pas acheminé vers un autre groupe de ponts dans ASA, et le trafic doit quitter ASA avant d'être acheminé par un routeur externe vers un autre groupe de ponts dans ASA. Bien que les fonctions de pont soient distinctes pour chaque groupe de ponts, de nombreuses autres fonctions sont partagées entre tous les groupes de ponts. Par exemple, tous les groupes

de ponts partagent une configuration de serveur syslog ou de serveur AAA. Pour une séparation complète des politiques de sécurité, utilisez les contextes de sécurité avec un groupe de ponts dans chaque contexte.

Vous pouvez inclure plusieurs interfaces par groupe de ponts. Consultez Lignes directrices sur le mode pare-feu, à la page 208 pour connaître le nombre exact de groupes de ponts et d'interfaces pris en charge. Si vous utilisez plus de deux interfaces par groupe de ponts, vous pouvez contrôler la communication entre plusieurs segments du même réseau, et pas seulement entre l'intérieur et l'extérieur. Par exemple, s'il y a trois segments internes avec lesquels vous ne souhaitez pas communiquer, vous pouvez placer chaque segment sur une interface distincte et les autoriser uniquement à communiquer avec l'interface externe. Vous pouvez également personnaliser les règles d'accès entre les interfaces pour autoriser uniquement les accès souhaités.

La figure suivante montre deux réseaux connectés à un ASA, qui comporte deux groupes de ponts.

Illustration 23 : Réseau de pare-feu transparent avec deux groupes de ponts

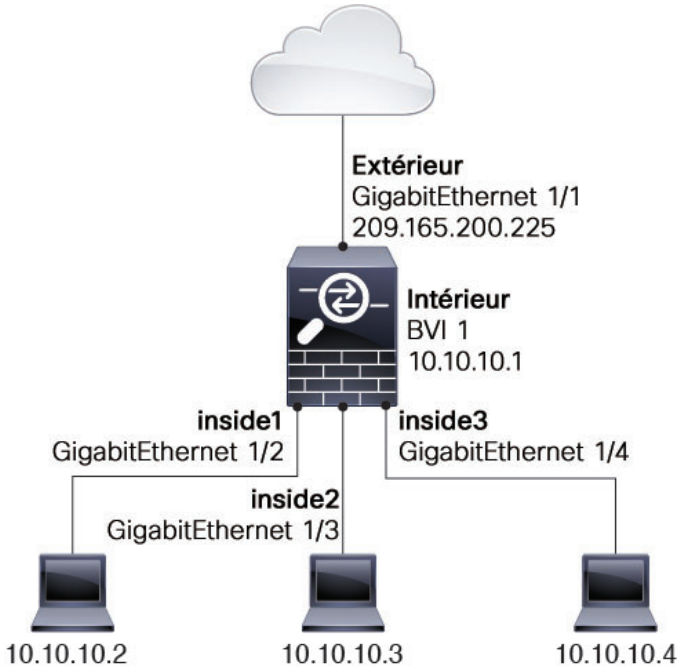


Groupes de ponts en mode pare-feu routé

Le trafic de groupe de ponts peut être acheminé vers d'autres groupes de ponts ou interfaces routées. Vous pouvez choisir d'isoler le trafic de groupe de ponts en n'attribuant pas de nom à l'interface BVI pour le groupe de ponts. Si vous nommez les BVI, alors les BVI participent au routage comme toute autre interface standard.

Une des utilisations d'un groupe de ponts en mode routé est d'utiliser des interfaces supplémentaires sur ASA au lieu d'un commutateur externe. Par exemple, la configuration par défaut de certains périphériques inclut une interface externe en tant qu'interface standard, puis toutes les autres interfaces affectées au groupe de ponts internes. Comme le but de ce groupe de ponts est de remplacer un commutateur externe, vous devez configurer une politique d'accès afin que toutes les interfaces du groupe de ponts puissent communiquer librement. Par exemple, comme dans la configuration par défaut, réglez toutes les interfaces au même niveau de sécurité, puis activez la communication de l'interface de même sécurité; aucune règle d'accès n'est requise.

Illustration 24 : Réseau de pare-feu routé avec un groupe de ponts interne et une interface de routage externe



Transmission du trafic non autorisée en mode routé

En mode routé, certains types de trafic ne peuvent pas traverser l'ASA, même si vous l'autorisez dans un critère d'accès. Le groupe de ponts peut toutefois autoriser la quasi-totalité du trafic à passer en utilisant un critère d'accès (pour le trafic IP) ou une règle EtherType (pour le trafic non IP) :

- Trafic IP : en mode de pare-feu routé, le trafic de diffusion et de multidiffusion est bloqué même si vous l'autorisez dans un critère d'accès, y compris les protocoles de routage dynamique non pris en charge et le protocole DHCP (sauf si vous configurez le relais DHCP). Dans un groupe de ponts, vous pouvez autoriser ce trafic avec un critère d'accès (à l'aide d'une ACL étendue).
- Trafic non IP : AppleTalk, IPX, BPDU et MPLS, par exemple, peuvent être configurés pour passer par une règle EtherType.

Remarque Le groupe de ponts ne transmet pas les paquets CDP ni les paquets qui n'ont pas d'EtherType valide supérieur ou égal à 0x600. Une exception est faite pour les BPDU et IS-IS, qui sont pris en charge.

Autorisation du trafic de couche 3

- Le trafic IPv4 et IPv6 de monodiffusion est autorisé par le groupe de ponts automatiquement d'une interface à sécurité supérieure vers une interface à sécurité inférieure, sans règle d'accès.
- Pour le trafic de couche 3 passant d'une interface de sécurité faible à une interface de sécurité élevée, une règle d'accès est requise sur l'interface de sécurité faible.

- Les protocoles ARP sont autorisés dans le groupe de ponts dans les deux sens sans règle d'accès. Le trafic ARP peut être contrôlé par inspection ARP.
- Les paquets de découverte de voisin IPv6 et de sollicitation de routeur peuvent être transmis à l'aide de règles d'accès.
- Le trafic en diffusion et en multidiffusion peut être transmis à l'aide de règles d'accès.

Adresses MAC autorisées

Les adresses MAC de destination suivantes sont autorisées par le biais du groupe de ponts si elles le sont par votre politique d'accès (voir Autorisation du trafic de couche 3, à la page 203). Toute adresse MAC qui ne figure pas dans cette liste est abandonnée.

- VRAIE adresse MAC de destination de diffusion égale à FFFF.FFFF.FFFF
- Adresses MAC IPv4 de multidiffusion, de 0100.5E00.0000 à 0100.5EFE.FFFF
- Adresses MAC IPv6 de multidiffusion, de 3333.0000.0000 à 3333.FFFF.FFFF
- Adresse de multidiffusion BPDU égale à 0100.0CCC.CCCD
- Adresses MAC AppleTalk de multidiffusion, de 0900.0700.0000 à 0900.07FF.FFFF

BPDU Handling (gestion des paquets BPDU)

Pour éviter les boucles avec le protocole Spanning Tree, les BPDU (Bridge Protocol Data Unit, Unité de données du protocole de pont) sont transmises par défaut. Pour bloquer les BPDU, vous devez configurer une règle EtherType pour les refuser. Vous pouvez également bloquer les BPDU sur les commutateurs externes. Par exemple, vous pouvez bloquer des BPDU sur le commutateur si des membres du même groupe de ponts sont connectés aux ports de commutation de différents VLAN. Dans ce cas, les BPDU d'un VLAN seront visibles dans l'autre VLAN, ce qui peut causer des problèmes de processus de sélection du pont racine du protocole Spanning Tree.

Si vous utilisez le basculement, vous souhaiterez peut-être bloquer les BPDU pour empêcher le port de commutation de passer à l'état de blocage lorsque la topologie change. Consultez Exigences en matière de groupes de ponts pour le basculement, à la page 284 pour de plus amples renseignements.

Recherches d'adresse MAC ou de route

Pour le trafic à l'intérieur d'un groupe de ponts, l'interface sortante d'un paquet est déterminée en effectuant une recherche d'adresse MAC de destination plutôt qu'une recherche de route.

Cependant, les recherches de routage sont nécessaires dans les situations suivantes :

- Trafic provenant de l'ASA : ajoutez une voie de routage statique/par défaut sur l'ASA pour le trafic destiné à un réseau distant où se trouve un serveur syslog, par exemple.
- Trafic de voix sur IP (VoIP) et TFTP avec inspection activée, et le point terminal se trouve à au moins un saut (ajouter une route statique sur l'ASA pour le trafic destiné au point terminal distant afin que les connexions secondaires soient réussies. L'ASA crée un « trou » temporaire dans la politique de contrôle d'accès pour autoriser la connexion secondaire; et comme la connexion peut utiliser un ensemble d'adresses IP différent de celui de la connexion principale, l'ASA doit effectuer une recherche de routage pour installer le sténopé sur la bonne interface.

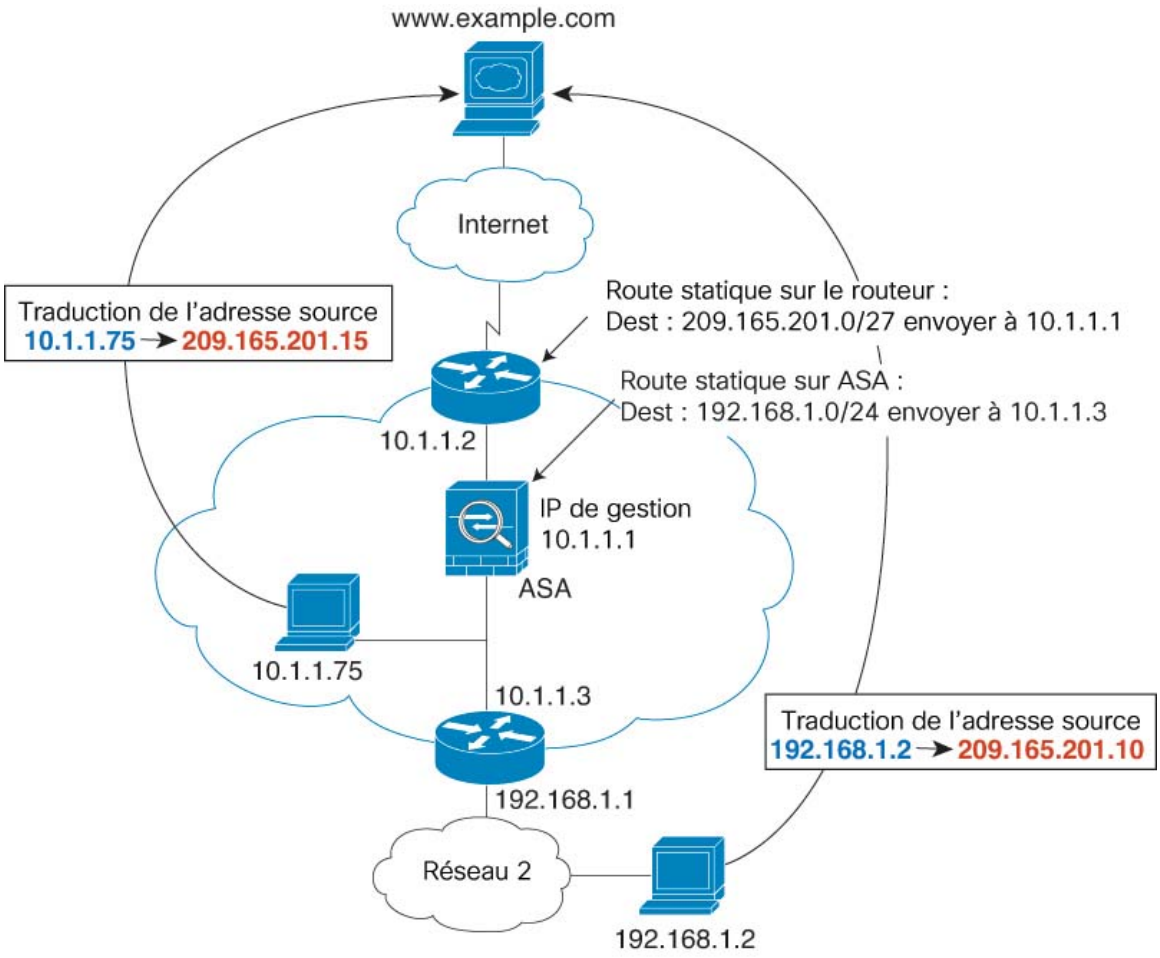
  Parmi les autres applications concernées, on trouve :

- CTIQBE
- GTP
- H.323
- MGCP
- RTSP
- SIP
- Skinny (SCCP)
- SQL*Net
- SunRPC
- TFTP

- Trafic à au moins un saut de distance pour lequel l'ASA exécute la NAT - Configurer une route statique sur l'ASA pour le trafic destiné au réseau distant. Vous avez également besoin d'une route statique sur le routeur en amont pour que le trafic destiné aux adresses mappées soit envoyé à l'ASA.

  Cette exigence de routage est également vraie pour les adresses IP intégrées pour VoIP et DNS avec inspection et NAT activées, et les adresses IP intégrées sont à au moins un sautillement. L'ASA doit identifier la bonne interface de sortie pour pouvoir effectuer la traduction.

Illustration 25 : Exemple de NAT : NAT dans un groupe de pont



Fonctionnalités non prises en charge pour les groupes de ponts en mode transparent

Le tableau suivant répertorie les fonctionnalités non prises en charge dans les groupes de ponts en mode transparent.

Tableau 4 : Fonctionnalités non prises en charge en mode transparent

Fonctionnalités	Description
DNS dynamique	—
Serveur sans état DHCPv6	Seul le serveur DHCPv4 est pris en charge sur les interfaces membres des groupes de ponts.
Relais DHCP	Le pare-feu transparent peut servir de serveur DHCPv4, mais il ne prend pas en charge le relais DHCP. Le relais DHCP n'est pas nécessaire, car vous pouvez permettre au trafic DHCP de passer en utilisant deux règles d'accès : une qui autorise les requêtes DHCP de l'interface interne vers l'extérieur et une qui autorise les réponses du serveur dans l'autre sens.

Fonctionnalités	Description
Protocoles de routage dynamique	Vous pouvez, cependant, ajouter des routes statiques pour le trafic provenant des interfaces ASA pour les membres des groupes de ponts. Vous pouvez également autoriser les protocoles de routage dynamique à l'aide de ASA en utilisant une règle d'accès.
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'ASA en l'autorisant dans une règle d'accès.
Qualité de service	—
Terminaison VPN pour le trafic traversant	Le pare-feu transparent prend en charge les tunnels VPN de site à site pour les connexions de gestion uniquement sur les interfaces membres des groupes de ponts. Il ne met pas fin aux connexions VPN pour le trafic passant par ASA. Vous pouvez faire passer le trafic VPN par l'ASA à l'aide d'un critère d'accès, mais cela ne met pas fin aux connexions hors gestion.
Communications unifiées	—

Fonctionnalités non prises en charge pour les groupes de ponts en mode routé

Le tableau suivant répertorie les fonctions non prises en charge dans les groupes de ponts en mode routé.

Tableau 5 : Fonctionnalités non prises en charge en mode routé

Fonctionnalités	Description
Interfaces membre EtherChannel ou VNI	Seules les interfaces physiques et les sous-interfaces sont prises en charge en tant qu'interfaces de membres de groupes de ponts. Les interfaces Management (gestion) ne sont pas non plus prises en charge.
Mise en grappe	Les groupes de ponts ne sont pas pris en charge dans la mise en grappe.
DNS dynamique	—
Serveur sans état DHCPv6	Seul le serveur DHCPv4 est pris en charge sur les BVI.
Relais DHCP	Le pare-feu routé peut servir de serveur DHCPv4, mais il ne prend pas en charge le relais DHCP sur les BVI ou les interfaces membres de groupes de ponts.
Protocoles de routage dynamique	Vous pouvez, cependant, ajouter des routes statiques pour les BVI. Vous pouvez également autoriser les protocoles de routage dynamique à l'aide de ASA en utilisant une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage dynamique.
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'ASA en l'autorisant dans une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage de multidiffusion.
Mode contexte multiple	Les groupes de ponts ne sont pas pris en charge en mode contexte multiple.

Fonctionnalités	Description
Qualité de service	Les interfaces sans groupe de ponts prennent en charge la QoS.
Terminaison VPN pour le trafic traversant	Vous ne pouvez pas mettre fin à une connexion VPN sur les BVI. Les interfaces qui ne font pas partie d'un groupe de pont prennent en charge le VPN. Les interfaces membres des groupes de ponts prennent en charge les tunnels VPN de site à site pour les connexions de gestion uniquement. Il ne met pas fin aux connexions VPN pour le trafic passant par ASA. Vous pouvez faire passer le trafic VPN par le groupe de ponts à l'aide d'une règle d'accès, mais cela ne met pas fin aux connexions hors gestion. Le VPN SSL sans client n'est pas non plus pris en charge.
Communications unifiées	Les interfaces de groupe hors pont prennent en charge les communications unifiées.

Paramètres d'usine

Mode par défaut

Le mode par défaut est le mode routé.

Valeurs par défaut des groupes de ponts

Par défaut, tous les paquets ARP sont transmis au sein du groupe de ponts.

Lignes directrices sur le mode pare-feu

Directives relatives au mode contextuel

Définissez le mode de pare-feu par contexte.

Directives de groupe de ponts (modes transparent et routé)

- Vous pouvez créer jusqu'à 250 groupes de ponts, avec interfaces par groupe de ponts.
- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- L'ASA ne prend pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.
- Une adresse IP pour les BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par ASA. Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d'hôte (255.255.255.255).

- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- Pour l'ASAv50 sur VMware avec des interfaces ixgbevf pontées, le mode transparent n'est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Dans le cas du Firepower 1010, il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.
- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.
- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la ASA comme passerelle par défaut.
- En mode transparent, la voie de routage *par défaut*, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.
- Le protocole PPPoE n'est pas pris en charge sur l'interface Management (gestion).
- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par ASA et VNI ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de ASA lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de l'ASA exécutant BFD, alors l'ASA abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

Directives et limites additionnelles

- Lorsque vous modifiez les modes de pare-feu, l'ASA efface la configuration en cours, car de nombreuses commandes ne sont pas prises en charge pour les deux modes. La configuration de démarrage reste inchangée. Si vous rechargez sans enregistrer, la configuration de démarrage est chargée et le mode revient aux paramètres d'origine. Consultez Définir le mode du pare-feu, à la page 210 pour en savoir plus sur la sauvegarde de votre fichier de configuration.
- Si vous téléchargez une configuration de texte sur l'ASA qui modifie le mode avec la commande **firewall transparent** , veillez à placer la commande en haut de la configuration; l'ASA change de mode dès qu'il lit la commande, puis continue de lire la configuration que vous avez téléchargée. Si la commande apparaît ultérieurement dans la configuration, l'ASA efface toutes les lignes précédentes de cette dernière. Consultez Définir l'image ASA, ASDM et la configuration de démarrage, à la page 1350 pour en savoir plus sur le téléchargement de fichiers texte.

Définir le mode du pare-feu

Cette section décrit comment changer de mode de pare-feu.

Remarque Nous vous recommandons de définir le mode de pare-feu avant d'effectuer toute autre configuration, car la modification de ce dernier efface la configuration en cours.

Avant de commencer

Lorsque vous changez de mode, l'ASA efface la configuration en cours (voir Lignes directrices sur le mode pare-feu, à la page 208 pour plus d'informations).

- Si vous avez déjà une configuration remplie, assurez-vous de sauvegarder votre configuration avant de modifier le mode. vous pouvez utiliser cette sauvegarde comme référence lors de la création de votre nouvelle configuration. Voir Sauvegarde et restauration de configurations ou d'autres fichiers, à la page 1353.
- Utilisez l'interface de ligne de commande du port de console pour changer de mode. Si vous utilisez tout autre type de session, y compris l'outil de l'interface de ligne de commande ASDM ou SSH, vous serez déconnecté lorsque la configuration sera effacée et vous devrez vous reconnecter à l'ASA en utilisant le port de console dans tous les cas.
- Définissez le mode dans le contexte.

Remarque Pour définir le mode de pare-feu à transparent et également configurer l'accès de gestion ASDM après avoir effacé la configuration, consultez Configurer l'accès ASDM, à la page 18.

Procédure

Définissez le mode de pare-feu sur transparent :

Pare-feu transparent

Exemple :

```
ciscoasa(config)# firewall transparent
```

Pour changer le mode à routé, saisissez la commande **no firewall transparent** (pas de pare-feu transparent).

Remarque
Vous n'êtes pas invité à confirmer le changement de mode de pare-feu; la modification se produit immédiatement.

Exemples de mode de pare-feu

Cette section comprend des exemples illustrant la manière dont le trafic circule à travers l'ASA en mode de pare-feu routé et transparent.

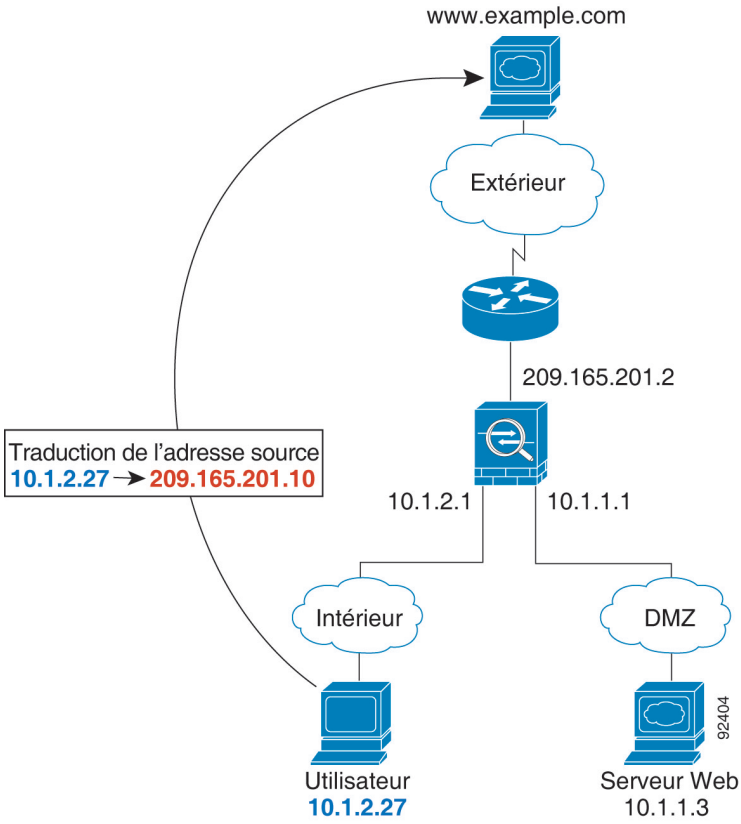
Progression des données dans l'ASA en mode de pare-feu routé

Les sections suivantes décrivent comment les données passent par l'ASA en mode de pare-feu routé dans plusieurs scénarios.

Un utilisateur interne visite un serveur web

La figure suivante montre un utilisateur interne accédant à un serveur web externe.

Illustration 26 : De l'intérieur vers l'extérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. L'utilisateur sur le réseau interne demande une page Web à www.exemple.com.
2. L'ASA reçoit le paquet et, comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.

3. L'ASA traduit l'adresse réelle (10.1.2.27) en adresse mappée 209.165.201.10, qui se trouve sur le sous-réseau de l'interface externe.

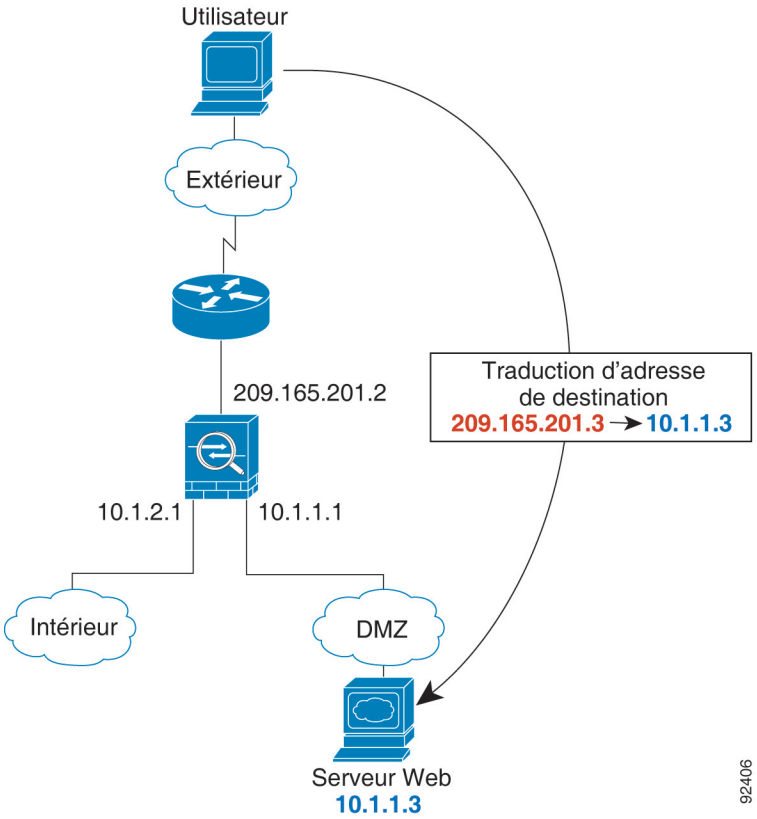
   L'adresse mappée peut se trouver sur n'importe quel sous-réseau, mais le routage est simplifié lorsqu'elle se trouve sur le sous-réseau d'interface externe.

4. L'ASA enregistre ensuite qu'une session est établie et transfère le paquet de l'interface externe.
5. Lorsque www.exemple.com répond à la demande, le paquet passe par l'ASA, et comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion. L'ASA effectue la NAT en ne traduisant pas l'adresse de destination globale en adresse d'utilisateur locale, 10.1.2.27.
6. L'ASA transmet le paquet à l'utilisateur interne.

Un utilisateur externe visite un serveur web sur la DMZ

La figure suivante montre un utilisateur externe accédant au serveur web DMZ.

Illustration 27 : Externe vers DMZ



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe demande une page Web au serveur web DMZ en utilisant l'adresse mappée 209.165.201.3, qui se trouve sur le sous-réseau de l'interface externe.
2. L'ASA reçoit le paquet et traduit l'adresse mappée en adresse réelle 10.1.1.3.

3. Comme il s'agit d'une nouvelle session, l'ASA vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

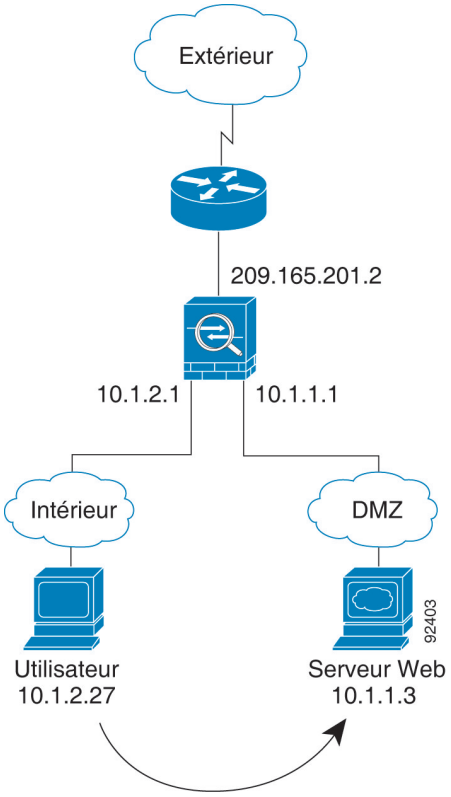
   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.

4. L'ASA ajoute ensuite une entrée de session au chemin rapide et transfère le paquet de l'interface DMZ.
5. Lorsque le serveur web DMZ répond à la demande, le paquet passe par l'ASA et, comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion. L'ASA effectue la NAT en traduisant l'adresse réelle en 209.165.201.3.
6. L'ASA transmet le paquet à l'utilisateur externe.

Un utilisateur interne visite un serveur web sur la DMZ

La figure suivante montre un utilisateur interne accédant au serveur web DMZ.

Illustration 28 : Interne à DMZ



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau interne demande une page Web au serveur web DMZ en utilisant l'adresse de destination 10.1.1.3.
2. L'ASA reçoit le paquet et, comme il s'agit d'une nouvelle session, l'ASA vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.

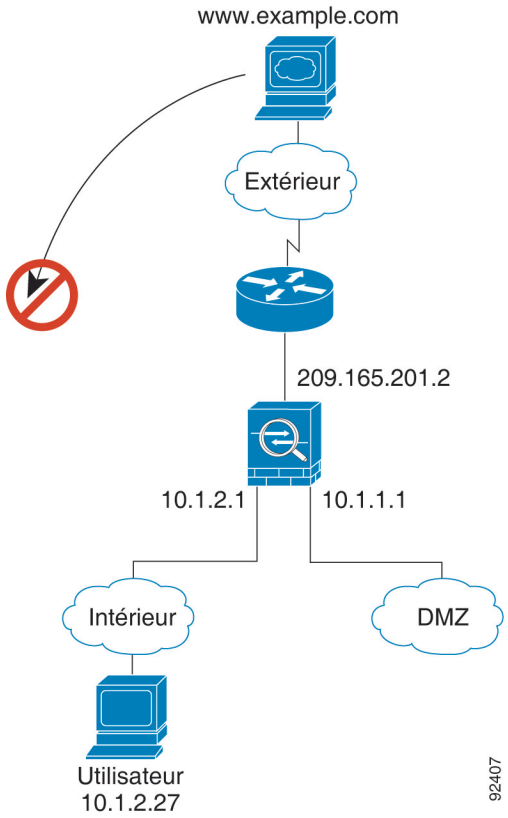
3. L'ASA enregistre ensuite qu'une session est établie et transfère le paquet de l'interface DMZ.

4. Lorsque le serveur web DMZ répond à la demande, le paquet emprunte le chemin d'accès rapide, ce qui lui permet de contourner les nombreuses recherches associées à une nouvelle connexion.
5. L'ASA transmet le paquet à l'utilisateur interne.

Un utilisateur externe tente d'accéder à un hôte interne

La figure suivante montre un utilisateur externe qui tente d'accéder au réseau interne.

Illustration 29 : De l'extérieur vers l'intérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe tente d'atteindre un hôte interne (en supposant que l'hôte a une adresse IP routable).

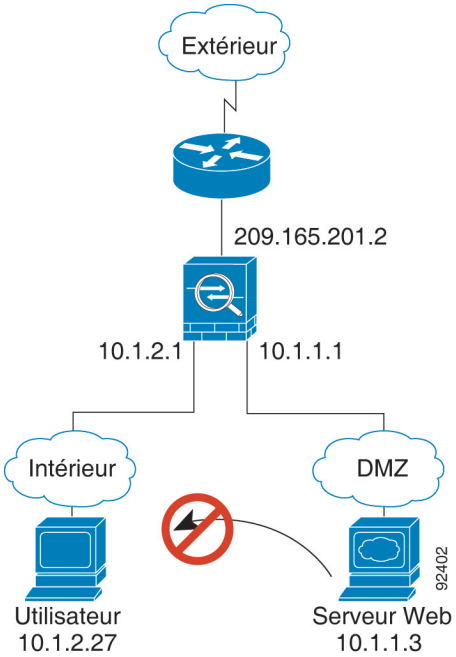
   Si le réseau interne utilise des adresses privées, aucun utilisateur externe ne peut atteindre le réseau interne sans la NAT. L'utilisateur externe peut tenter de joindre un utilisateur interne en utilisant une session NAT existante.
2. L'ASA reçoit le paquet et, parce qu'il s'agit d'une nouvelle session, il vérifie si le paquet est autorisé conformément à la politique de sécurité.
3. Le paquet est refusé et l'ASA abandonne le paquet et consigne la tentative de connexion.

   Si l'utilisateur externe tente d'attaque le réseau interne, l'ASA utilise de nombreuses technologies pour déterminer si un paquet est valide pour une session déjà établie.

Un utilisateur DMZ tente d'accéder à un hôte interne

La figure suivante montre un utilisateur dans la DMZ tente d'accéder au réseau interne.

Illustration 30 : DMZ vers interne



Les étapes suivantes décrivent comment les données passent par l'ASA :

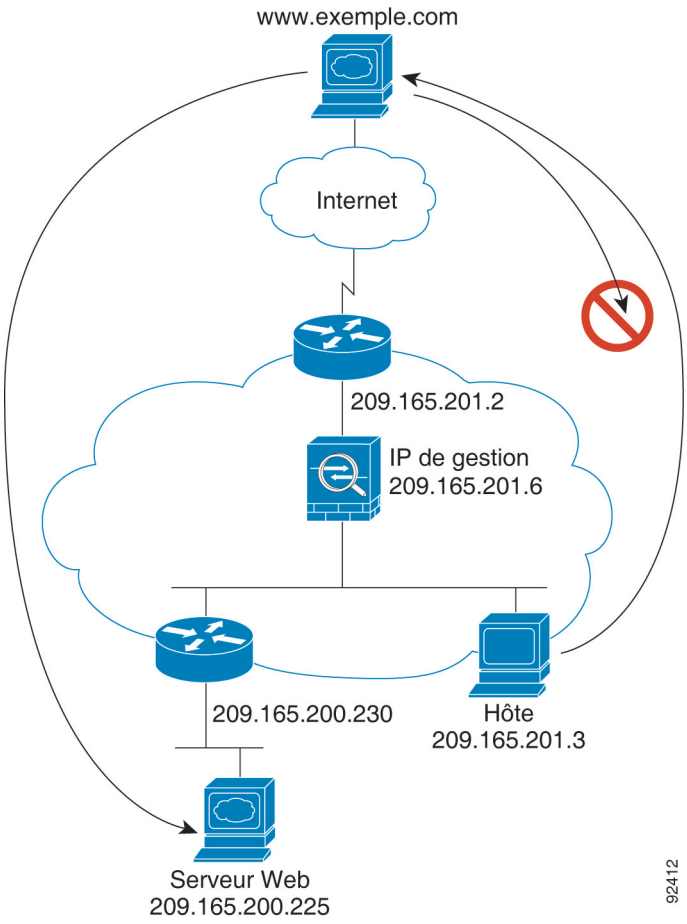
1. Un utilisateur sur le réseau DMZ tente d'atteindre un hôte interne. Étant donné que la DMZ n'a pas à acheminer le trafic sur Internet, le système d'adressage privé n'empêche pas le routage.
2. L'ASA reçoit le paquet et, parce qu'il s'agit d'une nouvelle session, il vérifie si le paquet est autorisé conformément à la politique de sécurité.

   Le paquet est refusé et l'ASA abandonne le paquet et consigne la tentative de connexion.

Progression des données dans le pare-feu transparent

La figure suivante montre une implémentation type de pare-feu transparent avec un réseau interne contenant un serveur Web public. L'ASA comporte un critère d'accès afin que les utilisateurs internes puissent accéder aux ressources Internet. Un autre critère d'accès permet aux utilisateurs externes d'accéder uniquement au serveur Web sur le réseau interne.

Illustration 31 : Chemin de données type d'un pare-feu transparent

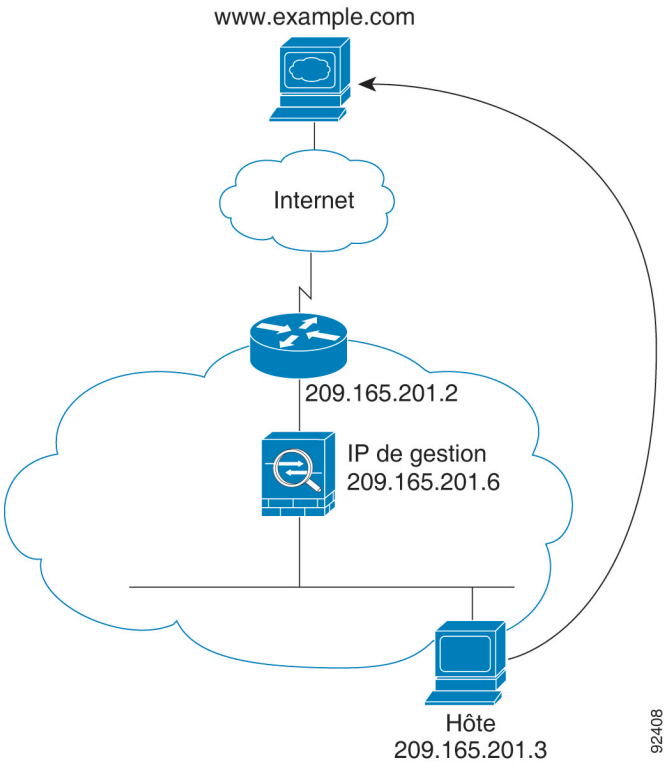


Les sections suivantes décrivent comment les données passent par l'ASA.

Un utilisateur interne visite un serveur web

La figure suivante montre un utilisateur interne accédant à un serveur web externe.

Illustration 32 : De l'intérieur vers l'extérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. L'utilisateur sur le réseau interne demande une page Web à www.exemple.com.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

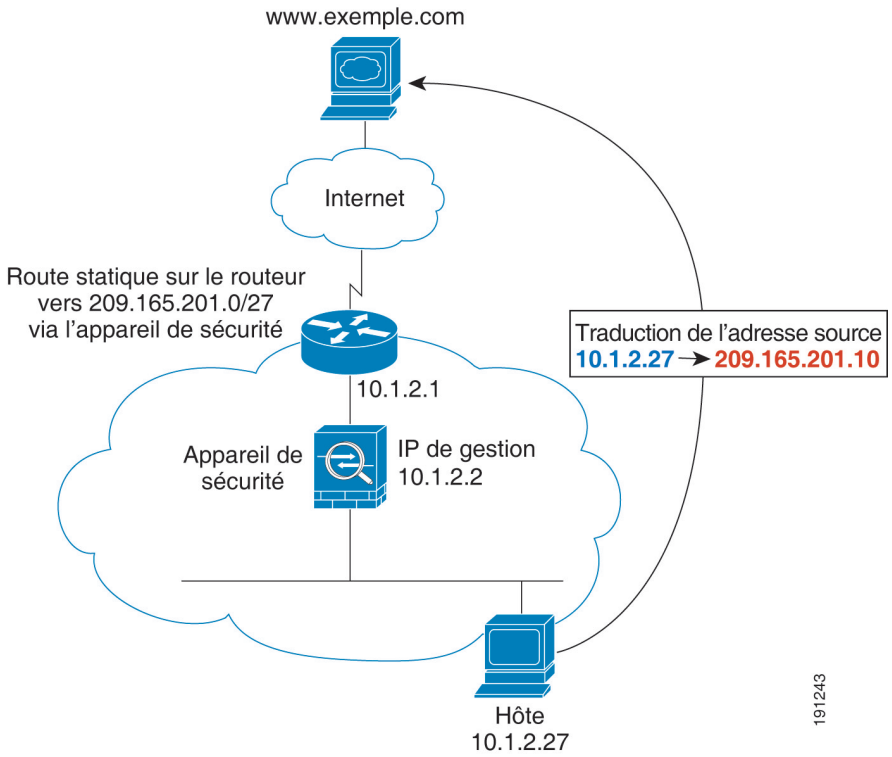
   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA enregistre qu'une session est établie.
4. Si l'adresse MAC de destination se trouve dans son tableau, l'ASA transfère le paquet hors de l'interface externe. L'adresse MAC de destination est celle du routeur en amont, 209.165.201.2.

   Si l'adresse MAC de destination ne se trouve pas dans le tableau ASA, il tente de découvrir l'adresse MAC en envoyant une requête ARP ou un message Ping. Le premier paquet est abandonné.
5. Le serveur web répond à la demande; comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion.
6. L'ASA transmet le paquet à l'utilisateur interne.

Un utilisateur interne visite un serveur web à l'aide de la NAT

La figure suivante montre un utilisateur interne accédant à un serveur web externe.

Illustration 33 : De l'intérieur à l'extérieur avec la NAT



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. L'utilisateur sur le réseau interne demande une page Web à www.exemple.com.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet selon une interface unique.
3. L'ASA traduit l'adresse réelle (10.1.2.27) en adresse mappée 209.165.201.10.

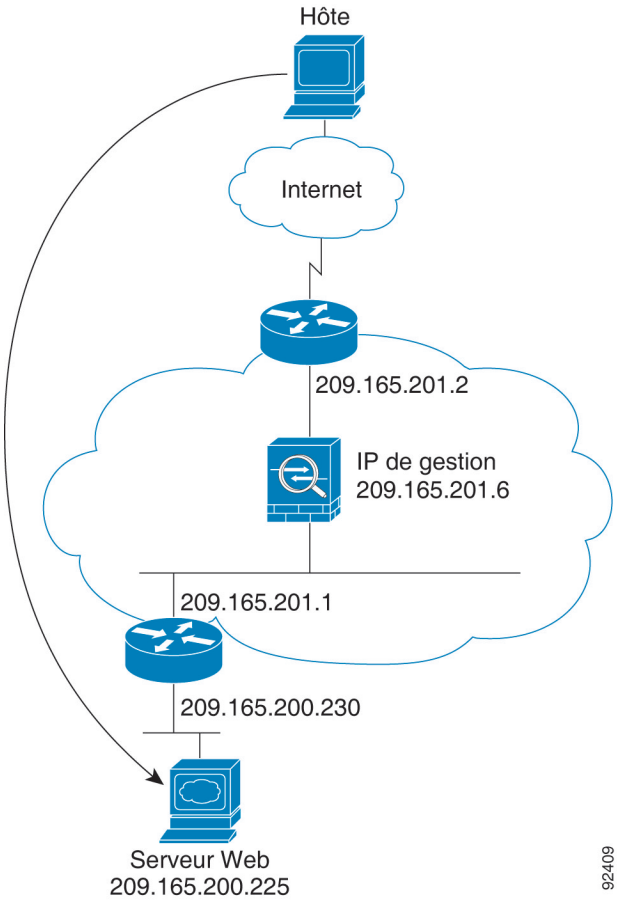
   Étant donné que l'adresse mappée ne se trouve pas sur le même réseau que l'interface externe, assurez-vous que le routeur en amont a une route statique vers le réseau mappé qui pointe vers l'ASA.
4. L'ASA enregistre ensuite qu'une session est établie et transfère le paquet de l'interface externe.
5. Si l'adresse MAC de destination se trouve dans son tableau, l'ASA transfère le paquet hors de l'interface externe. L'adresse MAC de destination est celle du routeur en amont, 10.1.2.1.

   Si l'adresse MAC de destination ne se trouve pas dans le tableau ASA, il tente alors de découvrir l'adresse MAC en envoyant une requête ARP et un message Ping. Le premier paquet est abandonné.
6. Le serveur web répond à la demande; comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion.
7. L'ASA effectue la NAT en ne traduisant pas l'adresse mappée en adresse réelle, 10.1.2.27.

Un utilisateur externe visite un serveur web sur le réseau interne

La figure suivante montre un utilisateur externe accédant au serveur web interne.

Illustration 34 : De l'extérieur vers l'intérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe demande une page Web au serveur web interne.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA enregistre qu'une session est établie.
4. Si l'adresse MAC de destination se trouve dans son tableau, l'ASA transfère le paquet hors de l'interface interne. L'adresse MAC de destination est celle du routeur en aval, 209.165.201.1.

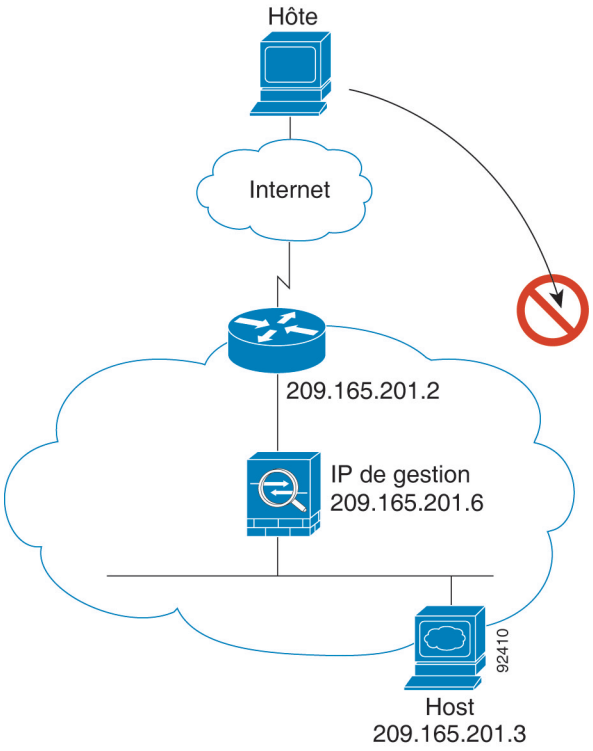
   Si l'adresse MAC de destination ne se trouve pas dans le tableau ASA, il tente alors de découvrir l'adresse MAC en envoyant une requête ARP et un message Ping. Le premier paquet est abandonné.
5. Le serveur web répond à la demande; comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion.

6. L'ASA transmet le paquet à l'utilisateur externe.

Un utilisateur externe tente d'accéder à un hôte interne

La figure suivante montre un utilisateur externe qui tente d'accéder à un hôte sur le réseau interne.

Illustration 35 : De l'extérieur vers l'intérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe tente d'atteindre un hôte interne.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. Le paquet est refusé, car aucun critère d'accès n'autorise l'hôte externe, et le ASA abandonne le paquet.
4. Si l'utilisateur externe tente d'attaque le réseau interne, l'ASA utilise de nombreuses technologies pour déterminer si un paquet est valide pour une session déjà établie.

Historique du mode de pare-feu

Tableau 6 : Historique des fonctionnalités du mode de pare-feu

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Mode de pare-feu transparent	7.0(1)	Un pare-feu transparent est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés. Nous avons introduit les commandes suivantes : **firewall transparent**, **show firewall**.
Groupes de ponts de pare-feu transparents	v 8.4(1)	Si vous ne souhaitez pas le surdébit des contextes de sécurité ou si vous souhaitez optimiser votre utilisation des contextes de sécurité, vous pouvez regrouper les interfaces dans un groupe de ponts, puis configurer plusieurs groupes de ponts, un pour chaque réseau. Le trafic de groupe de ponts est isolé des autres groupes de ponts. Vous pouvez configurer jusqu'à 8 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces au maximum par groupe de ponts. **Remarque** Bien que vous puissiez configurer plusieurs groupes de ponts sur l'ASA 5505, la restriction de 2 interfaces de données en mode transparent sur l'ASA 5505 signifie que vous ne pouvez utiliser efficacement qu'un seul groupe de ponts. Nous avons introduit les commandes suivantes : **interface bvi**, **bridge-group**, **show bridge-group**.
Prise en charge du mode de pare-feu mixte en mode de contexte multiple	8.5(1)/9.0(1)	Vous pouvez définir le mode de pare-feu indépendamment pour chaque contexte de sécurité en mode de contexte multiple, de sorte que certains puissent s'exécuter en mode transparent et que d'autres s'exécutent en mode routé. Nous avons modifié la commande suivante : **firewall transparent**.
Nombre maximum de groupes de ponts en mode transparent augmenté à 250	9.3(1)	Le nombre maximum de groupes de ponts est passé de 8 à 250 groupes de ponts. Vous pouvez configurer jusqu'à 250 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces maximum par groupe de ponts. Nous avons modifié les commandes suivantes : **interface bvi**, **bridge-group**.
Nombre maximum d'interfaces en mode transparent par groupe de ponts augmenté à 64	9.6(2)	Le nombre maximum d'interfaces par groupe de ponts est passé de 4 à 64. Nous n'avons pas modifié de commandes.

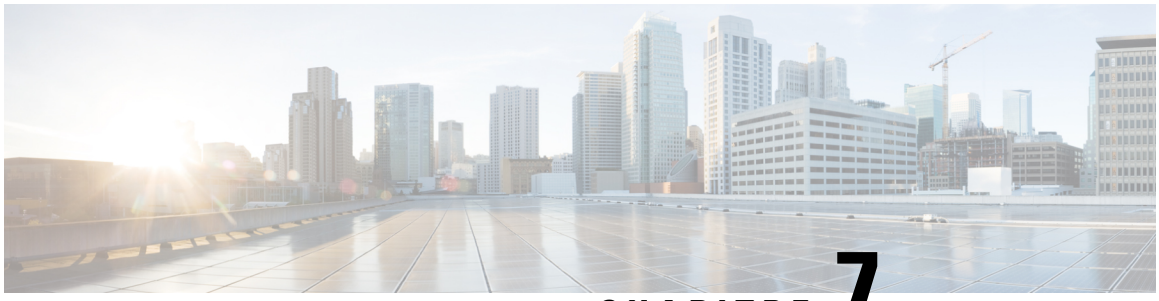
Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage et pont intégrés	9.7(1)	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que l'ASA relie par des ponts au lieu de routes. L'ASA n'est pas un vrai pont, car l'ASA continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur l'ASA à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : mode de contexte multiple, mise en grappe d'ASA. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Nous avons modifié les commandes suivantes : **access-group, access-list ethertype, arp-inspection, dhcpd, mac-address-table static, mac-address-table aging-time, mac-learn, route, show arp-inspection, show bridge-group, show mac-address-table, show mac-learn**
Prise en charge du déploiement en mode transparent pour un dispositif logique Firepower 4100/9300 ASA	9.10(1)	Vous pouvez désormais spécifier le mode transparent ou routé lorsque vous déployez l'ASA sur un Firepower 4100/9300 Commandes FXOS nouvelles ou modifiées : **enter bootstrap-key FIREWALL_MODE**, **set value routed**, **set value transparent**



PARTIE II

Fonctionnalités de haute disponibilité et d'évolutivité

- Mode contexte multiple, à la page 225
- Basculement pour la haute disponibilité, à la page 273
- Basculement pour la haute disponibilité dans le nuage public, à la page 331
- Grappe ASA pour le Secure Firewall 3100, à la page 353
- Grappe ASA pour le Firepower 4100/9300, à la page 445
- Grappe ASA pour l'ASA virtuel pour le cloud privé, à la page 545
- Grappe ASA pour l'ASA virtuel dans un nuage public, à la page 615



CHAPITRE 7

Mode contexte multiple

Ce chapitre décrit comment configurer plusieurs contextes de sécurité sur l'ASA.

- À propos des contextes de sécurité, à la page 225
- Licences pour le mode de contexte multiple, à la page 237
- Conditions préalables pour le mode de contexte multiple, à la page 238
- Lignes directrices pour le mode de contexte multiple, à la page 238
- Paramètres par défaut du mode de contexte multiple, à la page 239
- Configurer plusieurs contextes, à la page 239
- Changer entre les contextes et l'espace d'exécution du système, à la page 251
- Gérer les contextes de sécurité, à la page 252
- Supervision des contextes de sécurité, à la page 256
- Exemples de mode de contexte multiple, à la page 267
- Historique du mode de contexte multiple, à la page 268

À propos des contextes de sécurité

Vous pouvez partitionner un ASA unique en plusieurs périphériques virtuels, appelés contextes de sécurité. Chaque contexte agit comme un périphérique indépendant, avec sa politique de sécurité, ses interfaces et ses administrateurs. Les contextes multiples sont similaires au fait d'avoir plusieurs périphériques autonomes. Pour les fonctionnalités non prises en charge en mode de contexte multiple, consultez Lignes directrices pour le mode de contexte multiple, à la page 238.

Cette section fournit un aperçu des contextes de sécurité.

Utilisations courantes des contextes de sécurité

Vous pouvez utiliser plusieurs contextes de sécurité dans les situations suivantes :

- Vous êtes un fournisseur de services et vous souhaitez vendre des services de sécurité à de nombreux clients. En activant plusieurs contextes de sécurité sur l'ASA, vous pouvez mettre en œuvre une solution économique et peu encombrante qui sépare et sécurise tout le trafic client, tout en facilitant la configuration.
- Vous êtes une grande entreprise ou un campus universitaire et souhaitez séparer complètement les services.
- Vous êtes une entreprise qui souhaite fournir des politiques de sécurité distinctes à différents services.
- Vous avez un réseau qui nécessite plusieurs ASA.

Fichiers de configuration de contexte

Cette section décrit comment l'ASA met en œuvre les configurations en mode de contexte multiple.

Configurations de contexte

Pour chaque contexte, l'ASA comprend une configuration qui identifie la politique de sécurité, les interfaces et toutes les options que vous pouvez configurer sur un périphérique autonome. Vous pouvez stocker les configurations de contexte dans la mémoire flash ou vous pouvez les télécharger à partir d'un serveur TFTP, FTP ou HTTP(S).

Configuration système

L'administrateur du système ajoute et gère les contextes en configurant chaque emplacement de configuration de contexte, les interfaces allouées et d'autres paramètres de fonctionnement de contexte dans la configuration système, qui, à l'instar d'une configuration monomode, est la configuration de démarrage. La configuration système identifie les paramètres de base de l'ASA. La configuration système n'inclut aucune interface réseau ni aucun paramètre réseau pour elle-même; au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise l'un des contextes désigné comme *contexte d'administration*. La configuration système comprend une interface de basculement spécialisée pour le trafic de basculement uniquement.

Configuration du contexte d'administration

Le contexte d'administration est similaire à tout autre contexte, sauf que lorsqu'un utilisateur se connecte au contexte d'administration, cet utilisateur dispose de droits d'administrateur système et peut accéder au système et à tous les autres contextes. Le contexte admin n'est limité en aucune façon et peut être utilisé comme contexte standard. Cependant, comme la connexion au contexte admin vous accorde des privilèges d'administrateur sur tous les contextes, vous devrez peut-être restreindre l'accès au contexte admin aux utilisateurs appropriés. Le contexte d'administration doit résider dans la mémoire flash et non à distance.

Si votre système est déjà en mode de contexte multiple, ou si vous effectuez une conversion à partir du mode unique, le contexte d'administration est automatiquement créé sous la forme d'un fichier sur la mémoire flash interne, appelé admin.cfg. Ce contexte s'appelle « admin ». Si vous ne souhaitez pas utiliser admin.cfg comme contexte d'administration, vous pouvez modifier le contexte d'administration.

Classement des paquets par l'ASA

Chaque paquet qui entre dans le châssis doit être classé par l'ASA, de sorte que ce dernier puisse déterminer à quel contexte envoyer un paquet.



Remarque Si l'adresse MAC de destination est une adresse MAC de multidiffusion ou de diffusion, le paquet est dupliqué et remis à chaque contexte.

Critères de classificateurs valides

Cette section décrit les critères utilisés par le classificateur.

Remarque Pour le trafic de gestion destiné à une interface, l'adresse IP de l'interface est utilisée pour la classification.

La table de routage n'est pas utilisée pour la classification des paquets.

Interfaces uniques

Si un seul contexte est associé à l'interface d'entrée, l'ASA classe le paquet dans ce contexte. En mode de pare-feu transparent, des interfaces uniques pour les contextes sont requises. Cette méthode est donc utilisée pour classer les paquets à tout moment.

Adresses MAC uniques

Si plusieurs contextes partagent une interface, le classificateur utilise des adresses MAC uniques attribuées à l'interface dans chaque contexte. Un routeur en amont ne peut pas acheminer directement vers un contexte sans adresse MAC unique. Vous pouvez activer la génération automatique des adresses MAC. Vous pouvez également définir les adresses MAC manuellement lorsque vous configurez chaque interface.

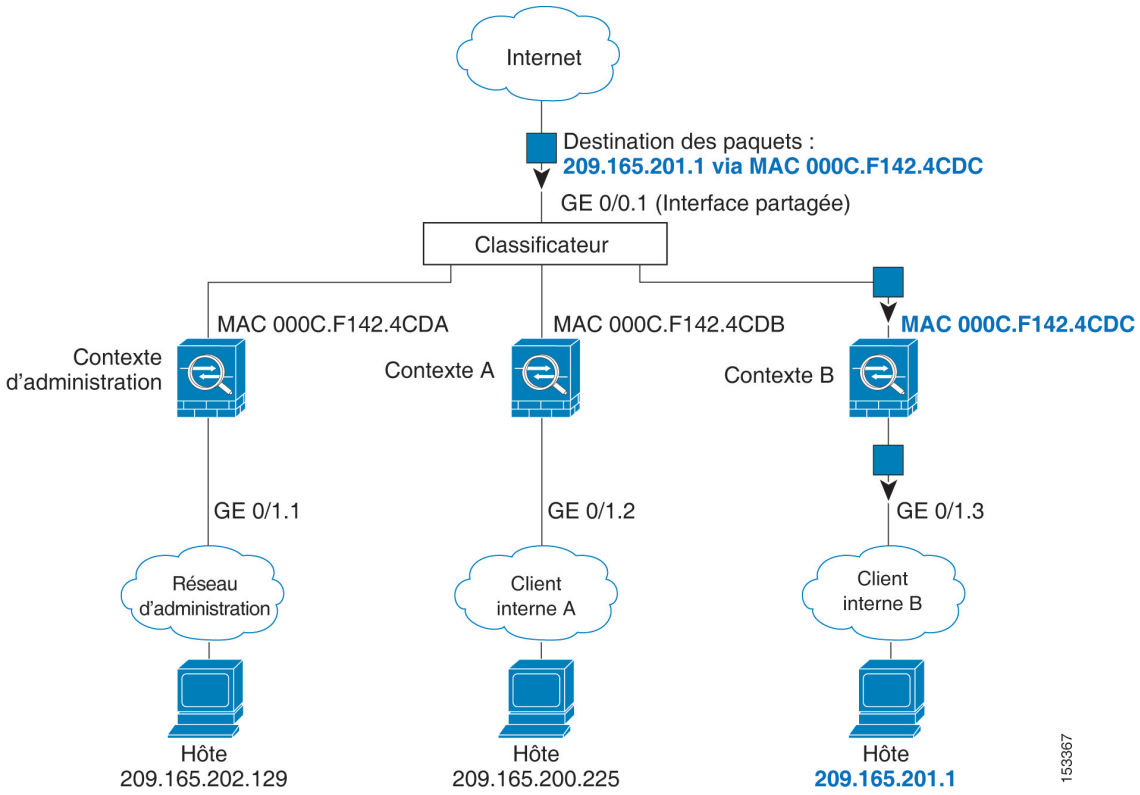
Configuration NAT

Si vous n'activez pas l'utilisation d'adresses MAC uniques, l'ASA utilise les adresses mappées dans votre configuration NAT pour classer les paquets. Nous vous conseillons d'utiliser des adresses MAC au lieu de NAT afin que la classification du trafic puisse avoir lieu indépendamment de l'exhaustivité de la configuration NAT.

Exemples de classement

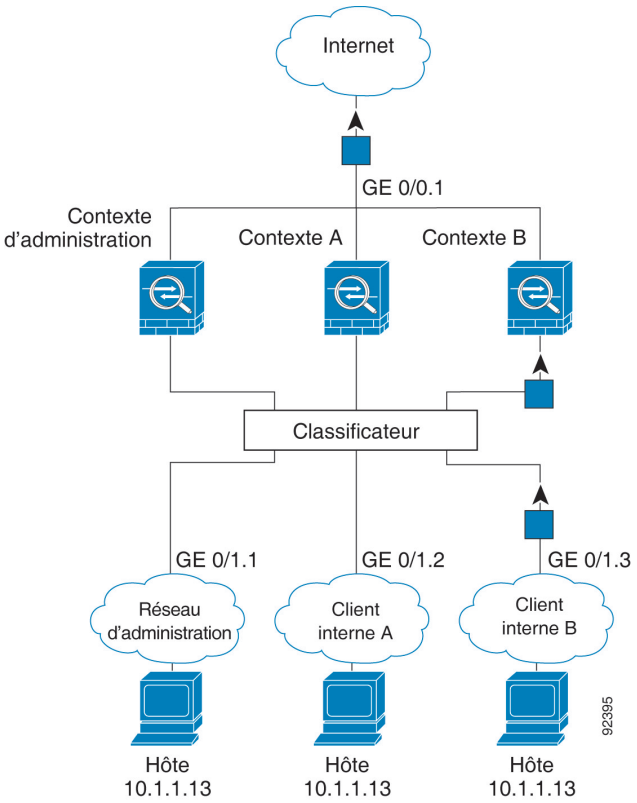
La figure suivante montre plusieurs contextes partageant une interface externe. Le classificateur affecte le paquet au contexte B, car le contexte B comprend l'adresse MAC à laquelle le routeur envoie le paquet.

Illustration 36 : Classification des paquets avec une interface partagée à l'aide d'adresses MAC



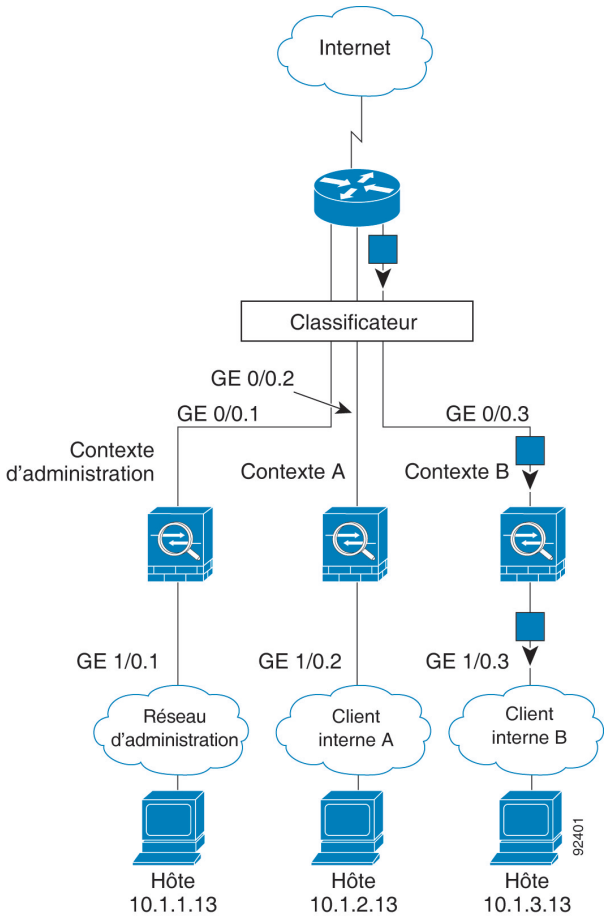
Notez que tout nouveau trafic entrant doit être classé, même en provenance des réseaux internes. La figure suivante montre un hôte sur le réseau interne du contexte B qui accède à Internet. Le classificateur affecte le paquet au contexte B, car l'interface d'entrée est Gigabit Ethernet 0/1.3, qui est affectée au contexte B.

Illustration 37 : Trafic entrant des réseaux internes



Pour les pare-feu transparents, vous devez utiliser des interfaces uniques. La figure suivante montre un paquet destiné à un hôte du contexte B à partir d'Internet. Le classificateur affecte le paquet au contexte B, car l'interface d'entrée est Gigabit Ethernet 1/0.3, qui est affectée au contexte B.

Illustration 38 : Contextes de pare-feu transparent



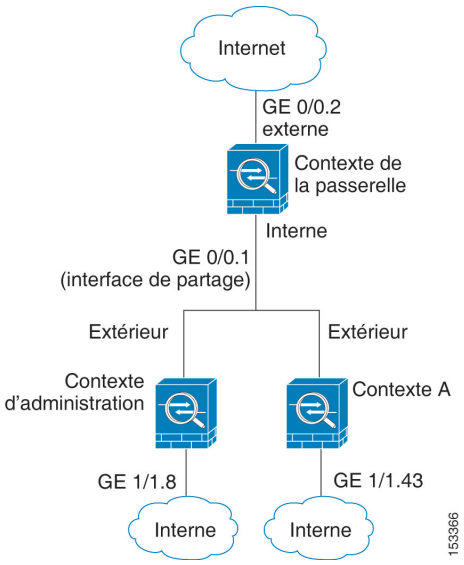
Contextes de sécurité en cascade

Le fait de placer un contexte directement devant un autre contexte s'appelle *des contextes en cascade*; l'interface externe d'un contexte est la même interface que l'interface interne d'un autre contexte. Vous pourriez souhaiter mettre des contextes en cascade si vous souhaitez simplifier la configuration de certains contextes en configurant des paramètres partagés dans le contexte supérieur.

Remarque La mise en cascade des contextes nécessite des adresses MAC uniques pour chaque interface de contexte. En raison des limites de la classification des paquets sur des interfaces partagées sans adresses MAC, nous vous conseillons de ne pas utiliser de contextes de chaîne de caractères sans adresses MAC uniques.

La figure suivante montre un contexte de passerelle avec deux contextes derrière la passerelle.

Illustration 39 : Contextes en cascade



Accès de gestion aux contextes de sécurité

L'ASA fournit un accès administrateur de système en mode de contexte multiple ainsi qu'un accès pour les administrateurs de contexte individuel.

Accès à l'administrateur système

Vous pouvez accéder à l'ASA en tant qu'administrateur système de deux manières :

- Accédez à la console ASA.

  À partir de la console, vous accédez à l'*espace d'exécution du système*, ce qui signifie que toutes les commandes que vous saisissez n'affectent que la configuration ou le fonctionnement du système (pour les commandes d'exécution).

- Accédez au contexte d'administration à l'aide de Telnet, SSH ou ASDM.

En tant qu'administrateur système, vous pouvez accéder à tous les contextes.

L'espace d'exécution du système ne prend en charge aucune commande AAA, mais vous pouvez configurer son propre mot de passe d'activation, ainsi que ses noms d'utilisateur dans la base de données locale pour fournir des connexions individuelles.

Accès à l'administrateur de contexte

Vous pouvez accéder à un contexte en utilisant Telnet, SSH ou ASDM. Si vous vous connectez à un contexte de non-administration, vous pouvez uniquement accéder à la configuration de ce contexte. Vous pouvez fournir des identifiants individuels pour le contexte.

Utilisation de l'interface de gestion

L'interface de gestion est une interface distincte uniquement pour le trafic de gestion.

En mode de pare-feu routé, vous pouvez partager l'interface de gestion dans tous les contextes.

En mode de pare-feu transparent, l'interface de gestion est spéciale. En plus du nombre maximal d'interfaces de trafic traversant autorisé, vous pouvez également utiliser l'interface de gestion en tant qu'interface de gestion uniquement distincte. Cependant, en mode contexte multiple, vous ne pouvez pas partager d'interfaces entre des contextes transparents. Vous pouvez plutôt utiliser les sous-interfaces de l'interface de gestion et en affecter une à chaque contexte. Cependant, seuls les modèles de périphérique Firepower autorisent les sous-interfaces sur l'interface de gestion. Pour les modèles d'ASA, vous devez utiliser une interface de données ou une sous-interface d'une interface de données et l'ajouter à un groupe de ponts dans le contexte.

Pour le contexte transparent Châssis Firepower 4100/9300 , ni l'interface de gestion ni la sous-interface ne conservent leur état spécial. Dans ce cas, vous devez la traiter comme une interface de données et l'ajouter à un groupe de ponts. (Notez qu'en mode contexte unique, l'interface de gestion conserve son état spécial.)

Une autre considération à propos du mode transparent : lorsque vous activez le mode à contextes multiples, toutes les interfaces configurées sont automatiquement affectées au contexte Admin. Par exemple, si votre configuration par défaut comprend l'interface de gestion, cette interface sera affectée au contexte d'administration. Une option consiste à laisser l'interface principale allouée au contexte d'administration et à la gérer à l'aide du VLAN natif, puis d'utiliser des sous-interfaces pour gérer chaque contexte. Gardez à l'esprit que si vous rendez le contexte d'administration transparent, son adresse IP sera supprimée. vous devez l'affecter à un groupe de ponts et affecter l'adresse IP aux BVI.

À propos de la gestion des ressources

Par défaut, tous les contextes de sécurité ont un accès illimité aux ressources de l'ASA, sauf lorsque des limites maximales par contexte sont appliquées; la seule exception concerne les ressources du VPN, qui sont désactivées par défaut. Si vous trouvez qu'un ou plusieurs contextes utilisent trop de ressources et qu'ils entraînent le refus de connexion à d'autres contextes, par exemple, vous pouvez configurer la gestion des ressources pour limiter l'utilisation des ressources par contexte. Pour les ressources VPN, vous devez configurer la gestion des ressources pour autoriser tous les tunnels VPN.

Classes des ressources

L'ASA gère les ressources en attribuant des contextes aux classes de ressources. Chaque contexte utilise les limites de ressources définies par la classe. Pour utiliser les paramètres d'une classe, affectez le contexte à la classe lorsque vous définissez le contexte. Tous les contextes appartiennent à la classe par défaut s'ils ne sont pas affectés à une autre classe; vous n'avez pas à attribuer activement un contexte à la classe par défaut. Vous ne pouvez affecter un contexte qu'à une seule classe de ressources. L'exception à cette règle est que les limites non définies dans la classe membre sont héritées de la classe par défaut; ainsi, un contexte peut être membre de la classe par défaut et d'une autre classe.

Limites des ressources

Vous pouvez définir la limite des ressources individuelles en pourcentage (s'il y a une limite de système matériel) ou en tant que valeur absolue.

Pour la plupart des ressources, l'ASA ne réserve pas une partie des ressources pour chaque contexte attribué à la classe; au lieu de cela, l'ASA définit la limite maximum pour un contexte. Si vous dépassez les ressources ou si vous permettez à certaines ressources d'être illimitées, quelques contextes peuvent « utiliser » ces ressources, ce qui peut affecter le service fourni à d'autres contextes. L'exception concerne les types de ressources VPN, que vous ne pouvez pas dépasser, de sorte que les ressources attribuées à chaque contexte sont garanties. Pour prendre en charge des rafales temporaires de sessions VPN au-delà de la quantité attribuée, l'ASA prend en charge un type de ressource VPN en « rafale », qui est égal au nombre de sessions VPN non

attribuées restantes. Les sessions en rafale *peuvent* être surexploitées et sont disponibles pour les contextes selon le principe du premier arrivé premier servi.

Classe par défaut

Tous les contextes appartiennent à la classe par défaut s'ils ne sont pas affectés à une autre classe; vous n'avez pas besoin d'affecter activement un contexte à la classe par défaut.

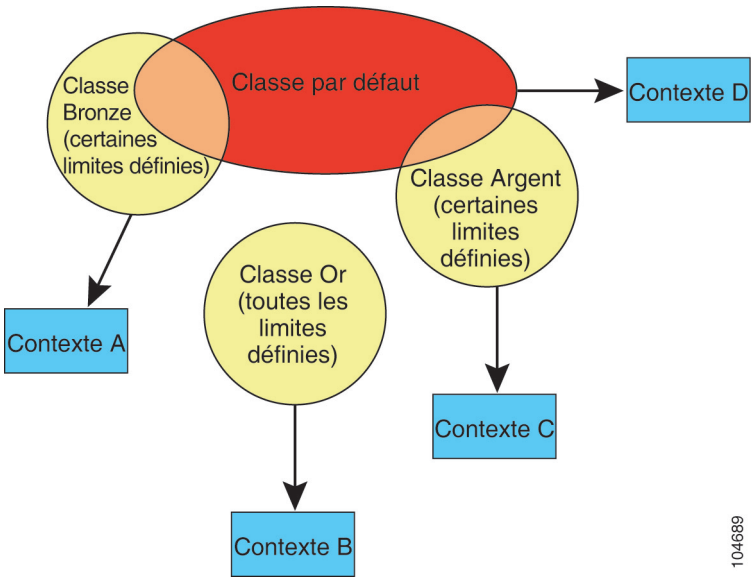
Si un contexte appartient à une autre classe que la classe par défaut, les paramètres de cette classe remplacent toujours les paramètres de la classe par défaut. Cependant, si l'autre classe a des paramètres non définis, le contexte membre utilise la classe par défaut pour ces limites. Par exemple, si vous créez une classe avec une limite de 2 % pour toutes les connexions simultanées, mais aucune autre limite, toutes les autres limites sont héritées de la classe par défaut. Inversement, si vous créez une classe avec une limite pour toutes les ressources, la classe n'utilise aucun paramètre de la classe par défaut.

Pour la plupart des ressources, la classe par défaut fournit un accès illimité aux ressources pour tous les contextes, sauf pour les limites suivantes :

- Sessions Telnet—5 sessions. (Le maximum par contexte.)
- Sessions SSH—5 sessions. (Le maximum par contexte.)
- Sessions ASDM—5 sessions. (Le maximum par contexte.)
- Adresses MAC—(selon le modèle). (Le maximum pour le système.)
- Secure Client (services client sécurisés) homologues—0 session. (Vous devez configurer manuellement la classe pour autoriser tous les homologues Secure Client (services client sécurisés).)
- Tunnels VPN de site à site—0 session. (Vous devez configurer manuellement la classe pour autoriser toutes les sessions VPN.)

La figure suivante montre la relation entre la classe par défaut et les autres classes. Les contextes A et C appartiennent à des classes avec des limites définies; les autres limites sont héritées de la classe par défaut. Le contexte B n'hérite aucune limite de la valeur par défaut, car toutes les limites sont définies dans sa classe, la classe Gold. Le contexte D n'a pas été affecté à une classe et est, par défaut, membre de la classe par défaut.

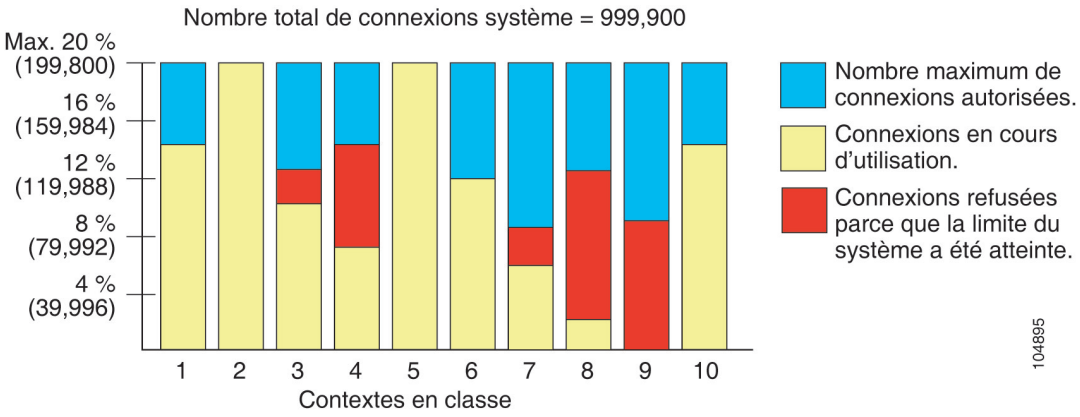
Illustration 40 : Classes des ressources



Utiliser des ressources surexploitées

Vous pouvez surabonner l'ASA en attribuant plus de 100 % d'une ressource dans tous les contextes (à l'exception des ressources VPN non rafales). Par exemple, vous pouvez définir la classe bronze pour limiter les connexions à 20 % par contexte, puis affecter 10 contextes à la classe pour un total de 200 %. Si les contextes utilisent simultanément plus que la limite du système, chaque contexte obtient moins des 20 % prévus.

Illustration 41 : Surabonnement des ressources

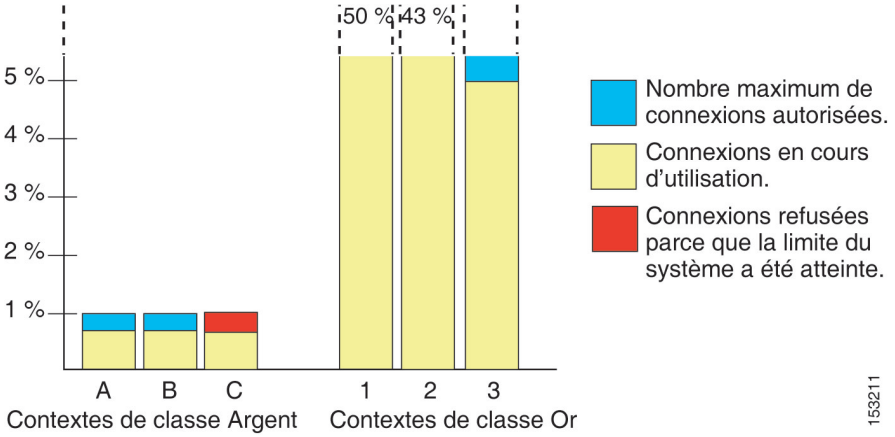


Utiliser des ressources illimitées

L'ASA vous permet d'attribuer un accès illimité à une ou plusieurs ressources dans une classe, au lieu d'un pourcentage ou d'un nombre absolu. Lorsqu'une ressource est illimitée, les contextes peuvent utiliser autant de ressources que le système en dispose. Par exemple, les contextes A, B et C appartiennent à la classe Silver, qui limite chaque membre de la classe à 1 % des connexions, pour un total de 3 %; mais les trois contextes n'utilisent actuellement que 2 % combinés. La classe Gold dispose d'un accès illimité aux connexions. Les

contextes de la classe Gold peuvent utiliser plus de 97 % des connexions « non attribuées »; ils peuvent également utiliser le 1 % de connexions non actuellement utilisées par les contextes A, B et C, même si cela signifie que les contextes A, B et C ne peuvent pas atteindre leur limite combinée de 3 %. La configuration d'un accès illimité s'apparente au surabonnement de l'ASA, à la différence que vous avez moins de contrôle sur le nombre de surabonnements du système.

Illustration 42 : Ressources illimitées



À propos des adresses MAC

Vous pouvez affecter manuellement des adresses MAC pour remplacer la valeur par défaut. Pour le mode de contexte multiple, vous pouvez générer automatiquement des adresses MAC uniques (pour toutes les interfaces affectées à un contexte) et un mode de contexte unique (pour les sous-interfaces)..

Remarque Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de liaison IPv6 sont générées sur la base de l'adresse MAC, l'attribution d'adresses MAC uniques aux sous-interfaces permet d'obtenir des adresses locales de liaison IPv6 uniques, ce qui peut éviter la perturbation du trafic dans certaines instances du périphérique ASA.

Adresses MAC en mode de contexte multiple

L'adresse MAC est utilisée pour classer les paquets dans un contexte. Si vous partagez une interface, mais que vous n'avez pas d'adresses MAC uniques pour l'interface dans chaque contexte, d'autres méthodes de classification sont tentées qui pourraient ne pas fournir une couverture complète.

Pour permettre aux contextes de partager des interfaces, vous devez activer la génération automatique d'adresses MAC virtuelles pour chaque interface de contexte partagé.

Adresses MAC automatiques

En mode de contexte multiple, la génération automatique affecte des adresses MAC uniques à toutes les interfaces affectées à un contexte.

Si vous attribuez manuellement une adresse MAC et activez la génération automatique, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée, si elle est activée.

Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC pour l'interface.

Comme les adresses générées automatiquement (lors de l'utilisation d'un préfixe) commencent par A2, vous ne pouvez pas commencer les adresses MAC manuelles par A2 si vous souhaitez également utiliser la génération automatique.

Le châssis génère l'adresse MAC en utilisant le format suivant :

A2*xx.yyzz.zzzz*

Où *xx.yy* est un préfixe défini par l'utilisateur ou un préfixe généré automatiquement en fonction des deux derniers octets de l'adresse MAC de l'interface, et *zz.zzzz* est un compteur interne généré par l'ASA. Pour l'adresse MAC de secours, l'adresse est identique, sauf que le compteur interne est augmenté de 1.

Pour donner un exemple d'utilisation du préfixe, si vous définissez le préfixe 77, l'ASA convertit 77 en valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native de l'ASA :

A2**4D.00***zz.zzzz*

Pour un préfixe 1009 (03F1), l'adresse MAC est :

A2**F1.03***zz.zzzz*

Remarque Le format d'adresse MAC sans préfixe est une version existante. Consultez la commande **mac-address auto** dans la référence de commandes pour plus d'informations sur le format existant.

Prise en charge du VPN

Pour les ressources VPN, vous devez configurer la gestion des ressources pour autoriser tous les tunnels VPN.

Vous pouvez utiliser le VPN de site à site en mode de contexte multiple.

Pour le VPN d'accès à distance, vous devez utiliser AnyConnect 3.x ou une version ultérieure pour le SSL VPN et le protocole IKEv2. Vous pouvez personnaliser le stockage flash par contexte pour les images et les personnalisations Secure Client (services client sécurisés), et utiliser la mémoire flash partagée pour tous les contextes. Pour les fonctionnalités non prises en charge, consultez Lignes directrices pour le mode de contexte multiple, à la page 238. Pour une liste détaillée des fonctionnalités VPN prises en charge par version ASA, consultez Historique du mode de contexte multiple, à la page 268.

Remarque La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante.

Licences pour le mode de contexte multiple

Modèle	Exigence de licence
Firepower 1010	Aucune assistance.
Firepower 1100	Licence Essentials : 2 contextes. *Licence facultative, maximum :* *Firepower 1120 : 5* *Firepower 1140 : 10* *Firepower 1150 : 25*
Firepower de la série 2100	Licence Essentials : 2 contextes. *Licence facultative, maximum :* *Firepower 2110 : 25* *Firepower 2120 : 25* *Firepower 2130 : 30* *Firepower 2140 : 40*
Secure Firewall 3100	Licence Essentials : 2 contextes. *Licence facultative, maximum :* *Secure Firewall 3105 : 100* *Secure Firewall 3110 : 100* *Secure Firewall 3120 : 100* *Secure Firewall 3130 : 100* *Secure Firewall 3140 : 100*
Firepower 4100	Licence Essentials : 10 contextes. *Licence facultative : jusqu'à 250 contextes.*
Firepower 9300	Licence Essentials : 10 contextes. *Licence facultative : jusqu'à 250 contextes.*
ISA 3000	Aucune assistance.
ASA virtuel	Aucune assistance.



Remarque Si le contexte d'administration ne contient que des interfaces de gestion uniquement et ne comprend aucune interface de données pour le trafic de transit, il n'est pas pris en compte dans la limite.

Remarque La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante.

Conditions préalables pour le mode de contexte multiple

Une fois que vous êtes en mode de contexte multiple, connectez-vous au système ou au contexte d'administration pour accéder à la configuration système. Vous ne pouvez pas configurer le système à partir d'un contexte de non-administration. Par défaut, après avoir activé le mode de contexte multiple, vous pouvez vous connecter au contexte d'administration en utilisant l'adresse IP de gestion par défaut.

Lignes directrices pour le mode de contexte multiple

Basculement

Le basculement en mode actif/actif n'est pris en charge qu'en mode de contexte multiple.

IPv6

Le routage IPv6 inter-contextes n'est pas pris en charge.

Fonctionnalités non prises en charge

Le mode de contexte multiple ne prend pas en charge les fonctionnalités suivantes :

- RIP
- OSPFv3. (OSPFv2 est pris en charge.)
- Routage multidiffusion
- Détection des menaces
- Communications unifiées
- Qualité de service
- Interfaces de tunnel virtuel (VTI)
- Suivi du routage statique

Le mode de contexte multiple ne prend actuellement pas en charge les fonctionnalités suivantes pour le VPN d'accès à distance :

- AnyConnect 2.x et versions antérieures
- IKEv1
- SAML
- Lancement Web

- Mise en correspondance VLAN
- Analyse de l'hôte
- Équilibrage de la charge VPN
- Personnalisation
- L2TP

Directives supplémentaires

- Le mode de contexte (unique ou multiple) n'est pas stocké dans le fichier de configuration, même s'il résiste aux redémarrages. Si vous devez copier votre configuration sur un autre périphérique, définissez le mode sur le nouveau périphérique pour qu'il corresponde.
- Si vous stockez les configurations de contexte dans le répertoire racine de la mémoire flash, sur certains modèles, vous risquez de manquer d'espace dans ce répertoire, même s'il y a de la mémoire disponible. Dans ce cas, créez un sous-répertoire pour vos fichiers de configuration. Arrière-plan : certains modèles utilisent le système de fichiers FAT 16 pour la mémoire flash interne, et si vous n'utilisez pas les noms abrégés conformes à la norme 8.3 ou les caractères majuscules, moins de 512 fichiers et dossiers peuvent être stockés parce que le système de fichiers utilise des logements pour stocker les noms de fichiers longs (voir http://support.microsoft.com/kb/120138/en-us).
- Dans ACI, le contrôle d'intégrité de la redirection basée sur les politiques (PBR) est exécuté (pings L2) en utilisant la même adresse MAC sur toutes les feuilles. Cela entraîne une oscillation MAC. Pour résoudre l'oscillation MAC, vous pouvez configurer l'option tap-mode sur l'ensemble en ligne. Cependant, si le Firewall Threat Defense à haute disponibilité est configuré, vous devez activer l'apprentissage MAC pour la gestion des connexions lors d'un basculement. Ainsi, dans un environnement ACI avec Firewall Threat Defense dans une paire à haute disponibilité utilisant des interfaces d'ensemble en ligne, pour éviter les pertes de paquet, déployez Firewall Threat Defense en mode autonome ou dans une grappe.

Paramètres par défaut du mode de contexte multiple

- Par défaut, l'ASA est en mode de contexte unique.
- Consultez Classe par défaut, à la page 233.

Configurer plusieurs contextes

Procédure

Étape 1 Activer ou désactiver le mode de contexte multiple, à la page 240.

Étape 2 (Facultatif) Configurer une classe pour la gestion des ressources, à la page 242

Remarque
Pour la prise en charge VPN, vous devez configurer des ressources VPN dans une classe de ressources; la classe par défaut n'autorise pas le VPN.

Étape 3 Configurez les interfaces dans l'espace d'exécution du système.

- Firepower 1100, Firepower 2100 en mode Appliance (appareil), Secure Firewall 3100 -Configuration de l'interface de base, à la page 671.
- Firepower 2100 en mode plateforme : consultez le guide de démarrage.
- Firepower 4100/9300—Périphériques logiques pour le Firepower 4100/9300, à la page 175

Étape 4 Configurer un contexte de sécurité, à la page 246.

Étape 5 (Facultatif) Attribuer automatiquement des adresses MAC aux interfaces de contexte, à la page 250

Étape 6 Terminez la configuration de l'interface dans le contexte. Consultez Interfaces en mode routage et en mode transparent, à la page 763.

Activer ou désactiver le mode de contexte multiple

Votre ASA est peut-être déjà configuré pour plusieurs contextes de sécurité selon la façon dont vous l'avez commandé auprès de Cisco. Si vous devez passer du mode unique au mode multiple, suivez les procédures de cette section.

Activer le mode de contexte multiple

Lorsque vous passez du mode unique au mode multiple, l'ASA convertit la configuration d'exécution en deux fichiers : une nouvelle configuration de démarrage qui comprend la configuration système et admin.cfg qui comprend le contexte d'administration (dans le répertoire racine de la mémoire flash interne). La configuration d'exécution d'origine est enregistrée sous le nom old_running.cfg (dans le répertoire racine de la mémoire flash interne). La configuration de démarrage d'origine n'est pas enregistrée. L'ASA ajoute automatiquement une entrée pour le contexte d'administration à la configuration système avec le nom « administration ».

Avant de commencer

Sauvegardez votre configuration de démarrage si elle diffère de la configuration d'exécution. Lorsque vous passez du mode unique au mode multiple, l'ASA convertit la configuration d'exécution en deux fichiers. La configuration de démarrage d'origine n'est pas enregistrée. Voir Sauvegarde et restauration de configurations ou d'autres fichiers, à la page 1353.

Procédure

Passez en mode de contexte multiple.

mode multiple

Exemple :

Vous êtes invité à changer de mode et à convertir la configuration, puis le système se recharge.

Remarque
Vous devrez régénérer la paire de clés RSA dans le contexte d'administration avant de pouvoir rétablir une connexion SSH. Dans la console, saisissez la commande **crypto key generate rsa modulus**. Consultez Configurer l'accès SSH, à la page 1275 pour de plus amples renseignements.

Exemple :

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#


***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system



***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

Rétablir le mode de contexte unique

Pour copier l'ancienne configuration en cours d'exécution dans la configuration de démarrage et changer le mode en mode unique, procédez comme suit.

Avant de commencer

Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Copiez la version de sauvegarde de votre configuration d'origine en cours d'exécution dans la configuration de démarrage actuelle :

copy disk0:old_running.cfg startup-config

Exemple :

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

Étape 2 Définissez le mode en mode unique :

mode unique

Exemple :

```
ciscoasa(config)# mode single
```

Vous êtes invité à redémarrer l'ASA.

Configurer une classe pour la gestion des ressources

Pour configurer une classe dans la configuration système, procédez comme suit. Vous pouvez modifier la valeur d'une limite de ressource particulière en entrant la commande avec une nouvelle valeur.

Avant de commencer

- Exécutez cette procédure dans l'espace d'exécution du système.
- Le tableau suivant répertorie les types de ressources et leurs limites. Consultez également la commande **show resource types**.

Remarque Si la limite du système est S.O., vous ne pouvez pas définir de pourcentage de la ressource, car il n'y a pas de limite de système stricte pour la ressource.

Tableau 7 : Noms et limites des ressources

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
asdm	Simultané	Au moins 1 5 au maximum	200	Sessions de gestion ASDM Les sessions ASDM utilisent deux connexions HTTPS: une pour la surveillance qui est toujours présente et une pour apporter des modifications de configuration qui est présente uniquement lorsque vous apportez des modifications. Par exemple, la limite système de 200 sessions ASDM représente une limite de 400 sessions HTTPS.

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
Connex.	Simultané ou taux	S. O.	Connexions simultanées : consultez Licences par modèle, à la page 149 pour connaître la limite de connexions disponibles correspondant à votre modèle. Taux : S.O.	Connexions TCP ou UDP entre deux hôtes, y compris les connexions entre un hôte et plusieurs autres hôtes. **Remarque** Des messages syslog sont générés pour la limite la plus basse, xlates ou conns. Par exemple, si vous définissez la limite de xlates à 7 et le conns à 9, alors l'ASA génère uniquement le message syslog 321001 (« Resource xlates » limite de 7 atteinte pour le contexte « ctx1 ») et non 321002 (« Resource « conn rate » limite de 5 atteinte pour le contexte « ctx1 »).
hôtes	Simultané	s.o.	s.o.	Les hôtes pouvant se connecter par l'intermédiaire de l'ASA.
Inspections	Taux	s.o.	s.o.	nombre d'inspections d'applications par seconde
mac-addresses	Simultané	S. O.	(varie selon le modèle)	Pour le mode de pare-feu transparent, le nombre d'adresses MAC autorisées dans le tableau d'adresses MAC.
routes	Simultané	s.o.	s.o.	routes dynamiques.
vpn burst anyconnect	Simultané	S. O.	Les homologues premium Secure Client (services client sécurisés) correspondant à votre modèle moins la somme des sessions attribuées à tous les contextes pour **vpn anyconnect**.	Le nombre de sessions Secure Client (services client sécurisés) autorisées au-delà de la quantité attribuée à un contexte avec **vpn anyconnect**. Par exemple, si votre modèle prend en charge 5 000 homologues et que vous affectez 4 000 homologues dans tous les contextes avec **vpn anyconnect**, les 1 000 sessions restantes sont disponibles pour **vpn burst anyconnect**. Contrairement à **vpn anyconnect**, qui garantit les sessions au contexte, le **vpn burst anyconnect** peut être surabonné; le groupement de rafales est disponible pour tous les contextes selon le principe du premier arrivé, premier servi.

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
vpn anyconnect	Simultané	S. O.	Consultez Licences par modèle, à la page 149 pour connaître les homologues Premium Secure Client (services client sécurisés) disponibles correspondant à votre modèle.	Homologues Secure Client (services client sécurisés). Vous ne pouvez pas surabonner cette ressource; toutes les affectations de contexte combinées ne peuvent pas dépasser la limite du modèle. Les homologues que vous affectez pour cette ressource sont garantis par le contexte.
vpn burst other	Simultané	S. O.	Le nombre de sessions Autre VPN correspondant à votre modèle moins la somme des sessions assignées à tous les contextes pour **vpn other**.	Le nombre de sessions VPN de site à site autorisées au-delà de la quantité attribuée à un contexte avec l'option **vpn other**. Par exemple, si votre modèle prend en charge 5 000 homologues et que vous affectez 4 000 homologues dans tous les contextes avec **vpn anyconnect**, les 1 000 sessions restantes sont disponibles pour **vpn burst anyconnect**. Contrairement à **vpn other**, qui garantit les sessions au contexte, **vpn burst other** peut être sursouscrit ; le groupement de rafales est disponible pour tous les contextes sur la base du premier arrivé, premier servi.
vpn other	Simultané	S. O.	Consultez Licences de fonctionnalités prises en charge par modèle, à la page 70 pour connaître les autres sessions VPN disponibles correspondant à votre modèle.	Sessions VPN de site à site. Vous ne pouvez pas surabonner cette ressource; toutes les affectations de contexte combinées ne peuvent pas dépasser la limite du modèle. Les sessions que vous affectez pour cette ressource sont garanties par le contexte.
ikEv1 en négociation	Simultané (pourcentage uniquement)	S. O.	Un pourcentage des autres sessions VPN attribuée à ce contexte. Consultez les ressources **vpn other** pour attribuer des sessions au contexte.	Négociations IKEv1 SA entrantes, en tant que pourcentage de la limite du contexte de l'autre VPN.
ssh	Simultané	Au moins 1 5 au maximum	100	Séances SSH.

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
stockage	Mo	Le maximum dépend du lecteur de mémoire flash que vous avez spécifié	Le maximum dépend du lecteur de mémoire flash que vous avez spécifié	Limite de stockage du répertoire de contexte en Mo. Spécifiez le lecteur à l'aide de la commande **storage-url**.
syslogs	Taux	s.o.	s.o.	Messages syslog par seconde.
telnet	Simultané	Au moins 1 5 au maximum	100	Sessions Telnet.
xlates	Simultané	s.o.	s.o.	Traduction d'adresses de réseau.

Procédure

Étape 1 Précisez le nom de la classe et accédez au mode de configuration de celle-ci :

class *name*

Exemple :

```
ciscoasa(config)# class gold
```

Le *name* (nom) est une chaîne de 20 caractères maximum. Pour définir les limites de la classe par défaut, saisissez « **default** » pour le nom.

Étape 2 Définir la limite de ressource pour un type de ressource :

limit-resource [**rate**] *resource_name number*[**%**]

Exemple :

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- Consultez le tableau précédent pour une liste des types de ressources. Si vous spécifiez **all**, toutes les ressources sont configurées avec la même valeur. Si vous spécifiez également une valeur pour une ressource particulière, la limite remplace la limite définie pour **all**.
- Saisissez l'argument **rate** pour définir le débit par seconde pour certaines ressources.
- Pour la plupart des ressources, spécifiez **0** comme *nombre* pour définir la ressource comme illimitée ou comme limite du système, le cas échéant. Pour les ressources VPN, la valeur **0** définit la limite à Aucun.
- Pour les ressources qui n'ont pas de limite système, vous ne pouvez pas définir le pourcentage (**%**). vous ne pouvez définir qu'une valeur absolue.

- Si vous définissez également la commande **quota management-session** dans un contexte pour définir le nombre maximal de sessions administratives (SSH, etc.), la valeur la plus basse sera utilisée.

Exemple

Par exemple, pour définir la limite de classe par défaut pour les connexions à 10 % au lieu d'illimité et pour autoriser 5 tunnels VPN de site à site avec 2 tunnels pour la rafale VPN, saisissez les commandes suivantes :

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

Toutes les autres ressources restent à illimité.

Pour ajouter une classe appelée gold, utilisez les commandes suivantes :

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

Lorsqu'un contexte est configuré avec une classe de ressources, une vérification est effectuée. Un avertissement est généré si les licences appropriées n'ont pas été installées avant les tentatives de connexion d'accès à distance VPN. L'administrateur doit ensuite obtenir une licence Secure Client Premier. Par exemple, un avertissement comme le suivant peut s'afficher :

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn anyconnect 10.0%
ciscoasa(config-class)# context test
Creating context 'text'...Done. (3)
ciscoasa(config-ctx)# member vpn
WARNING: Multi-mode remote access VPN support requires an AnyConnect Apex license.
Warning: An Access Context license is required for remote-access VPN support in multi-mode.
ciscoasa(config-ctx)#
```

Configurer un contexte de sécurité

La définition du contexte de sécurité dans la configuration système identifie le nom du contexte, l'URL du fichier de configuration, les interfaces qu'un contexte peut utiliser et d'autres paramètres.

Avant de commencer

- Exécutez cette procédure dans l'espace d'exécution du système.
- Configurer les interfaces. Pour les contextes en mode transparent, vous ne pouvez pas partager des interfaces entre les contextes, vous pouvez donc utiliser des sous-interfaces. Pour planifier l'utilisation de l'interface de gestion, consultez Utilisation de l'interface de gestion, à la page 231.
  - Firepower 1100, Firepower 2100 en mode Appliance (appareil), Secure Firewall 3100 -Configuration de l'interface de base, à la page 671.
  - Firepower 2100 en mode plateforme : consultez le guide de démarrage.
  - Firepower 4100/9300—Périphériques logiques pour le Firepower 4100/9300, à la page 175
- Si vous n'avez pas de contexte d'administration (par exemple, si vous effacez la configuration), vous devez d'abord préciser le nom du contexte d'administration en saisissant la commande suivante :

  ```
  ciscoasa(config)# admin-context name
  ```

  Bien que ce contexte n'existe pas encore dans votre configuration, vous pouvez par la suite entrer la commande « **context** *Name* » pour poursuivre la configuration du contexte d'administration.

Procédure

Étape 1 Ajouter ou modifier un contexte :

context *name*

Exemple :

```
ciscoasa(config)# context admin
```

Le *name* (nom) est une chaîne de 32 caractères maximum. Ce nom est sensible à la casse, vous pouvez donc avoir deux contextes nommés « clientA » et « ClientA », par exemple. Vous pouvez utiliser des lettres, des chiffres ou des tirets, mais vous ne pouvez pas commencer ou terminer le nom par un tiret.

Remarque
« System » ou « Null » (en lettres majuscules ou minuscules) sont des noms réservés et ne peuvent pas être utilisés.

Étape 2 (Facultatif) Ajoutez une description pour ce contexte :

description *texte*

Exemple :

```
ciscoasa(config-ctx)# description Admin Context
```

Étape 3 Précisez les interfaces que vous pouvez utiliser dans le contexte :

Pour allouer une interface :

allocate-interface *interface_id* [*mapped_name*] [**visible** | **invisible**]

Pour allouer une ou plusieurs sous-interfaces :

allocate-interface *interface_id.subinterface* [**-***interface_id.subinterface*] [*mapped_name*[**-***mapped_name*]] [**visible** | **invisible**]

Exemple :

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

Remarque
N'incluez pas d'espace entre le type d'interface et le numéro de port.

- Saisissez ces commandes plusieurs fois pour spécifier différentes plages. Si vous supprimez une allocation avec la forme **no** de cette commande, toutes les commandes de contexte qui incluent cette interface sont supprimées de la configuration en cours.
- Vous pouvez affecter les mêmes interfaces à plusieurs contextes en mode routé, si vous le souhaitez. Le mode transparent n'autorise pas les interfaces partagées.
- Le *mappé_name* (nom mapppé) est un alias alphanumérique pour l'interface qui peut être utilisé dans le contexte au lieu de l'ID de l'interface. Si vous ne spécifiez pas de nom mappé, l'ID d'interface est utilisé dans le contexte. Pour des raisons de sécurité, vous pouvez ne pas vouloir que l'administrateur de contexte sache quelles interfaces le contexte utilise. Un nom mappé doit commencer par une lettre, se terminer par une lettre ou un chiffre et avoir comme caractères internes uniquement des lettres, des chiffres ou un trait de soulignement. Par exemple, vous pouvez utiliser les noms suivants : **int0**, **inta**, **int_0**.
- Si vous spécifiez une plage de sous-interfaces, vous pouvez spécifier une plage correspondante de noms mappés. Suivez les directives suivantes concernant les plages :
  - Le nom mappé doit comprendre une partie alphabétique suivie d'une partie numérique. La partie alphabétique du nom mappé doit correspondre aux deux extrémités de la plage. Par exemple, saisissez la plage suivante : **int0-int10**. Si vous saisissez gig0/1.1-gig0/1.5 **happy**1-**sad**5, par exemple, la commande échoue.
  - La partie numérique du nom mappé doit inclure le même nombre de chiffres que la plage de la sous-interface. Par exemple, les deux plages comprennent 100 interfaces :**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100**. Si vous saisissez gig0/0.**100**-gig0/0.**199** int**1**-int**15**, par exemple, la commande échoue.
- Précisez **visible** pour voir le véritable ID de l'interface dans la commande **show interface** si vous définissez un nom mappé. Le mot clé par défaut **invisible** affiche uniquement le nom mappé.

Étape 4 Déterminez l'URL à partir de laquelle le système télécharge la configuration de contexte :

config-url *url*

Vous pouvez spécifier un fichier dans la mémoire flash ou sur un serveur distant.

Exemple :

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

Étape 5 (Facultatif) Autoriser chaque contexte à utiliser la mémoire flash pour stocker les paquets VPN, tels que Secure Client (services client sécurisés), ainsi que fournir le stockage pour Secure Client (services client sécurisés) SSL VPN sans client. Par exemple, si vous utilisez le mode de contexte multiple pour configurer un profil Secure Client (services client sécurisés) avec des politiques d'accès dynamique, vous devez planifier le stockage privé spécifique au contexte. Chaque contexte peut utiliser un espace de stockage privé ainsi qu'un espace de stockage partagé en lecture seule. **Remarque :** Assurez-vous que le répertoire cible est déjà présent sur le disque spécifié à l'aide de la commande **mkdir**.

storage-url {**private** | **shared**} [**disk***n***:/**]*path* [*context_label*]

Exemple :

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

Vous pouvez spécifier un espace de stockage **private** par contexte. Vous pouvez lire/écrire/supprimer à partir de ce répertoire dans le contexte (ainsi qu'à partir de l'espace d'exécution du système). Si vous ne spécifiez pas de numéro de disque, la valeur par défaut est disk0. Sous le *chemin* spécifié, ASA crée un sous-répertoire du nom du contexte. Par exemple, pour contexteA, si vous spécifiez **disk1:/private-storage** comme chemin, ASA crée un sous-répertoire pour ce contexte dans **disk1:/private-storage/contextA/**. Vous pouvez également éventuellement nommer le chemin dans le contexte avec une *context_label*, afin que le système de fichiers ne soit pas accessible aux administrateurs de contexte. Par exemple, si vous définissez la propriété *context_label* comme**context**, dans le contexte, ce répertoire s'appelle **context:**. Pour contrôler la quantité d'espace disque autorisée par contexte, consultez Configurer une classe pour la gestion des ressources, à la page 242.

Vous pouvez spécifier un espace de stockage **shared** en lecture seule par contexte, mais vous pouvez créer plusieurs répertoires partagés. Pour réduire la duplication de fichiers volumineux communs qui peuvent être partagés dans tous les contextes, tels que les paquets Secure Client (services client sécurisés), vous pouvez utiliser l'espace de stockage partagé. L'ASA ne crée pas de sous-répertoires de contexte pour cet espace de stockage, car il s'agit d'un espace partagé par plusieurs contextes. Seul l'espace d'exécution du système peut écrire et supprimer dans le répertoire partagé.

Étape 6 (Facultatif) Attribuez le contexte à une classe de ressources :

member *class_name*

Exemple :

```
ciscoasa(config-ctx)# member gold
```

Si vous ne spécifiez aucune classe, le contexte appartient à la classe par défaut. Vous ne pouvez affecter un contexte qu'à une seule classe de ressources.

Étape 7 (Facultatif) Attribuez un contexte à un groupe de basculement dans Basculement actif/Actif :

join-failover-group {**1** | **2**}

Exemple :

```
ciscoasa(config-ctx)# join-failover-group 2
```

Par défaut, les contextes sont dans le groupe 1. Le contexte d'administration doit toujours être dans le groupe 1.

Étape 8 (Facultatif) Activer Cloud Web Security pour ce contexte :

scansafe [**license** *key*]

Exemple :

```
ciscoasa(config-ctx)# scansafe
```

Si vous ne spécifiez pas de **license**, le contexte utilise la licence configurée dans la configuration système. L'ASA envoie la clé d'authentification aux serveurs mandataires de Cloud Web Security pour indiquer de quelle organisation provient la demande. La clé d'authentification est un nombre hexadécimal de 16 octets.

Consultez le guide de configuration du pare-feu pour obtenir des renseignements détaillés sur ScanSafe.

Exemple

L'exemple suivant définit le contexte d'administration sur « administrator », crée un contexte appelé « administrator » sur la mémoire flash interne, puis ajoute deux contextes d'un serveur FTP :

```
ciscoasa(config)# admin-context admin
ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

Attribuer automatiquement des adresses MAC aux interfaces de contexte

Cette section décrit comment configurer la génération automatique des adresses MAC. L'adresse MAC est utilisée pour classer les paquets dans un contexte.

Avant de commencer

- Lorsque vous configurez un de commande **« nameif »** pour l'interface dans un contexte, la nouvelle adresse MAC est générée immédiatement. Si vous activez cette fonctionnalité après avoir configuré les interfaces de contexte, les adresses MAC sont générées pour toutes les interfaces immédiatement après leur activation. Si vous désactivez cette fonctionnalité, l'adresse MAC par défaut de chaque interface

revient à l'adresse MAC. Par exemple, les sous-interfaces de GigabitEthernet 0/1 utilisent l'adresse MAC de GigabitEthernet 0/1.

- Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC de l'interface dans le contexte.

Procédure

Attribuez automatiquement des adresses MAC privées à chaque interface de contexte :

mac-address auto [**prefix** *prefix*]

Exemple :

```
ciscoasa(config)# mac-address auto prefix 19
```

Si vous n'écrivez pas de préfixe, l'ASA génère automatiquement ce dernier en fonction des deux derniers octets de l'.

Si vous saisissez manuellement un préfixe, le *préfixe* est une valeur décimale comprise entre 0 et 65 535. Ce préfixe est converti en nombre hexadécimal à quatre chiffres et utilisé dans l'adresse MAC.

Changer entre les contextes et l'espace d'exécution du système

Si vous vous connectez à l'espace d'exécution du système (ou au contexte d'administration), vous pouvez passer d'un contexte à l'autre et effectuer des tâches de configuration et de surveillance dans chaque contexte. La configuration en cours d'exécution que vous modifiez en mode de configuration ou qui est utilisée dans les commandes **de copie** ou **d'écriture** dépend de votre emplacement. Lorsque vous êtes dans l'espace d'exécution du système, la configuration en cours d'exécution se compose uniquement de la configuration système; lorsque vous êtes dans un contexte, la configuration en cours d'exécution comprend uniquement ce contexte. Par exemple, vous ne pouvez pas afficher toutes les configurations en cours d'exécution (système plus tous les contextes) en saisissant la commande **show running-config**. Seule la configuration actuelle s'affiche.

Procédure

Étape 1 Passez à un contexte :

changeto context *name*

L'invite passe à ciscoasa/*name*#

Étape 2 Passez à l'espace d'exécution du système :

changeto system

L'invite passe à ciscoasa#

Gérer les contextes de sécurité

Cette section décrit comment gérer les contextes de sécurité.

Supprimer un contexte de sécurité

Vous ne pouvez pas supprimer le contexte d'administration actuel, sauf si vous supprimez tous les contextes à l'aide de la commande **clear context**.

Remarque Si vous utilisez le basculement, il y a un délai entre le moment où vous supprimez le contexte sur l'unité active et le moment où le contexte est supprimé de l'unité en veille. Vous pourriez voir un message d'erreur indiquant que le nombre d'interfaces sur les unités actives et en veille n'est pas cohérent; cette erreur est temporaire et peut être ignorée.

Avant de commencer

Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Supprimez un seul contexte :

no context *name*

Toutes les commandes de contexte sont également supprimées. Le fichier de configuration de contexte n'est pas supprimé de l'emplacement de l'URL de configuration.

Étape 2 Supprimez tous les contextes (y compris le contexte d'administration) :

clear context

Les fichiers de configuration de contexte ne sont pas supprimés des emplacements des URL de configuration.

Modifier le contexte d'administration

La configuration système n'inclut aucune interface réseau ni aucun paramètre réseau pour elle-même; au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise l'un des contextes désigné comme contexte d'administration.

Le contexte d'administration est similaire à tout autre contexte, sauf que lorsqu'un utilisateur se connecte au contexte d'administration, cet utilisateur dispose de droits d'administrateur système et peut accéder au système et à tous les autres contextes. Le contexte admin n'est limité en aucune façon et peut être utilisé comme contexte standard. Cependant, comme la connexion au contexte admin vous accorde des privilèges d'administrateur sur tous les contextes, vous devrez peut-être restreindre l'accès au contexte admin aux utilisateurs appropriés.

Avant de commencer

- Vous pouvez définir n'importe quel contexte comme contexte d'administration, tant que le fichier de configuration est stocké dans la mémoire flash interne.
- Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Définissez le contexte d'administration :

admin-context *context_name*

Exemple :

```
ciscoasa(config)# admin-context administrator
```

Toutes les sessions de gestion à distance, telles que Telnet, SSH ou HTTPS, qui sont connectées au contexte d'administration sont terminées. Vous devez vous reconnecter au nouveau contexte d'administration.

Quelques commandes de configuration système, notamment **ntp server**, identifient un nom d'interface qui appartient au contexte d'administration. Si vous modifiez le contexte d'administration et que le nom de l'interface n'existe pas dans le nouveau contexte d'administration, veillez à mettre à jour toutes les commandes système qui font référence à l'interface.

Modifier l'URL du contexte de sécurité

Cette section décrit comment modifier l'URL du contexte.

Avant de commencer

- Vous ne pouvez pas modifier l'URL du contexte de sécurité sans recharger la configuration à partir de la nouvelle URL. L'ASA fusionne la nouvelle configuration avec la configuration en cours d'exécution.
- La saisie de la même URL fusionne également la configuration enregistrée avec la configuration d'exécution.
- Une fusion ajoute toutes les nouvelles commandes de la nouvelle configuration à la configuration en cours d'exécution.
  - Si les configurations sont identiques, aucune modification ne se produit.
  - Si des commandes sont en conflit ou si des commandes influent sur le fonctionnement du contexte, l'effet de la fusion dépend de la commande. Vous pourriez obtenir des erreurs ou des résultats inattendus. Si la configuration d'exécution est vide (par exemple, si le serveur n'est pas disponible et que la configuration n'a jamais été téléchargée), la nouvelle configuration est utilisée.
- Si vous ne souhaitez pas fusionner les configurations, vous pouvez effacer la configuration d'exécution, ce qui perturbe toute communication en raison du contexte, puis recharger la configuration à partir de la nouvelle URL.

- Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 (Facultatif, si vous ne souhaitez pas effectuer de fusion) Modifiez le contexte et effacez la configuration :

changeto context *name*

clear configure all

Exemple :

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(config)# clear configure all
```

Si vous souhaitez effectuer une fusion, passez à l'étape 2.

Étape 2 Passez à l'espace d'exécution du système :

changeto system

Exemple :

```
ciscoasa/ctx1(config)# changeto system
ciscoasa(config)#
```

Étape 3 Entrez en mode de configuration du contexte pour le contexte que vous souhaitez modifier.

context *name*

Exemple :

```
ciscoasa(config)# context ctx1
```

Étape 4 Saisissez la nouvelle URL. Le système charge immédiatement le contexte pour qu'il s'exécute.

config-url *new_url*

Exemple :

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

Recharger un contexte de sécurité

Vous pouvez recharger le contexte de deux manières :

- Effacez la configuration en cours d'exécution, puis importez la configuration de démarrage.

  Cette action efface la plupart des attributs associés au contexte, tels que les connexions et les tables NAT.
- Supprimez le contexte de la configuration système.

Cette action efface les attributs supplémentaires, tels que l'allocation de mémoire, qui pourraient être utiles pour le dépannage. Cependant, pour rajouter le contexte au système, vous devez redéfinir l'URL et les interfaces.

Recharger en effaçant la configuration

Procédure

Étape 1 Passez au contexte que vous souhaitez recharger :

changeto context *name*

Exemple :

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(comfig)#
```

Étape 2 Effacez la configuration d'exécution :

clear configure all

Cette commande efface toutes les connexions.

Étape 3 Rechargez la configuration :

copy startup-config running-config

Exemple :

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

L'ASA copie la configuration à partir de l'URL spécifiée dans la configuration système. Vous ne pouvez pas modifier l'URL à partir d'un contexte.

Recharger en supprimant et en rajoutant le contexte

Pour recharger le contexte en le supprimant, puis en le rajoutant, procédez comme suit.

Procédure

Étape 1 Supprimer un contexte de sécurité, à la page 252. **Also delete config URL file from the disk**

Étape 2 Configurer un contexte de sécurité, à la page 246

Supervision des contextes de sécurité

Cette section décrit comment afficher et superviser les renseignements contextuels.

Afficher les informations de contexte

À partir de l'espace d'exécution du système, vous pouvez afficher une liste de contextes, y compris le nom, les interfaces allouées et l'URL du fichier de configuration.

Procédure

Affichez tous les contextes :

show context [*name* | **detail**| **count**]

Si vous souhaitez afficher des renseignements pour un contexte particulier, spécifiez le *nom*.

L'option **detail** (détail) affiche des renseignements supplémentaires. Consultez les exemples de sortie ci-dessous suivants pour en savoir plus.

L'option **count** (nombre) affiche le nombre total de contextes.

Exemple

Voici un exemple de sortie de la commande **show context** . L'exemple de sortie suivant montre trois contextes :

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

Le tableau suivant affiche la description de chaque champ.

Tableau 8 : afficher les champs de contexte

Champ	Description
Nom du contexte	Répertorie tous les noms de contexte. Le nom du contexte avec l'astérisque (*) est le contexte d'administration.
Interfaces	Les interfaces attribuées au contexte.

Champ	Description
URL	L'URL à partir de laquelle l'ASA charge la configuration de contexte.

Voici un exemple de sortie de la commande **show context detail** :

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

Consultez la référence de commande pour en savoir plus sur la sortie **detail** (détail).

Voici un exemple de sortie de la commande **show context count** :

```
ciscoasa# show context count
Total active contexts: 2
```

Afficher l'affectation des ressources

À partir de l'espace d'exécution du système, vous pouvez afficher l'allocation pour chaque ressource pour toutes les classes et les membres de classe.

Procédure

Affichez l'allocation des ressources :

show resource allocation [**detail**]

Cette commande affiche l'allocation de ressources, mais n'affiche pas les ressources réelles utilisées. Consultez Afficher l'utilisation des ressources, à la page 260 pour de plus amples renseignements sur l'utilisation réelle des ressources.

L'argument **detail** affiche des renseignements supplémentaires. Consultez les exemples de sortie suivants pour en savoir plus.

Exemple

L'exemple de sortie suivant affiche l'allocation totale de chaque ressource en valeur absolue et en pourcentage des ressources système disponibles :

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Routes                      5000           N/A
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 AnyConnect                  1000           10%
 AnyConnectBurst              200           2%
 Other VPN Sessions            20           2.66%
 Other VPN Burst               20           2.66%
 All                    unlimited
```

Le tableau suivant affiche la description de chaque champ.

Tableau 9 : afficher les champs d'allocation de ressources

Champ	Description
Resource (Ressource)	Le nom de la ressource que vous pouvez limiter.
Total	La quantité totale de ressources allouées à tous les contextes. La quantité est un nombre absolu d'instances ou d'instances simultanées par seconde. Si vous avez spécifié un pourcentage dans la définition de la classe, l'ASA convertit le pourcentage en un nombre absolu pour cet affichage.
% of Avail (% de disponibilité)	Le pourcentage des ressources système totales allouées pour tous les contextes, si la ressource a une limite de système matériel. Si une ressource n'a pas de limite de système, cette colonne indique S.O.

L'exemple suivant illustre la sortie de la commande **show resource allocation detail** :

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
```

```
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Telnet           default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Routes           default          all       C  unlimited                N/A
                 gold               1       D  unlimited          5      N/A
                 silver             1      CA         10         10      N/A
                 bronze             0      CA          5                 N/A
                 All Contexts:      3                            20      N/A

Xlates           default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      23040      23040     N/A
                 bronze             0      CA      11520
                 All Contexts:      3                         23040     N/A

mac-addresses    default          all       C      65535
                 gold               1       D      65535      65535    100.00%
                 silver             1      CA       6553       6553      9.99%
                 bronze             0      CA       3276
                 All Contexts:      3                        137623    209.99%
```

Le tableau suivant affiche la description de chaque champ.

Tableau 10 : afficher les champs de détail de l'allocation des ressources

Champ	Description
Resource (Ressource)	Le nom de la ressource que vous pouvez limiter.
Classe	Le nom de chaque classe, y compris la classe par défaut. Le champ All contexts (Tous les contextes) affiche les valeurs totales pour toutes les classes.
Mmbrs (Membres)	Le nombre de contextes affectés à chaque classe.
Origin (Origine)	L'origine de la limite de ressources, comme suit : • R : vous définissez cette limite avec l'option **all** (toutes), plutôt qu'en tant que ressource individuelle. • C : cette limite est issue de la classe de membres. • D : cette limite n'a pas été définie dans la classe de membres, mais est issue de la classe par défaut. Pour un contexte attribué à la classe par défaut, la valeur sera « C » au lieu de « D ». L'ASA peut combiner « A » avec « C » ou « D ».
Limit (Limite)	La limite de la ressource par contexte, sous forme de nombre absolu. Si vous avez spécifié un pourcentage dans la définition de la classe, l'ASA convertit le pourcentage en un nombre absolu pour cet affichage.
Total	La quantité totale de ressources allouées à tous les contextes de la classe. La quantité est un nombre absolu d'instances ou d'instances simultanées par seconde. Si la ressource est illimitée, cet affichage est vide.
% of Avail (% de disponibilité)	Le pourcentage des ressources système totales allouées pour tous les contextes de la classe. Si la ressource est illimitée, cet affichage est vide. Si la ressource n'a pas de limite système, alors cette colonne indique S.O.

Afficher l'utilisation des ressources

À partir de l'espace d'exécution du système, vous pouvez afficher l'utilisation des ressources pour chaque contexte et afficher l'utilisation des ressources du système.

Procédure

Affichez l'utilisation des ressources pour chaque contexte :

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]

- Par défaut, **toute** l'utilisation des contextes est affichée; chaque contexte est répertorié séparément.

- Saisissez le mot clé **top** *n* pour afficher les contextes qui sont les *n* principaux utilisateurs de la ressource spécifiée. Vous devez spécifier un seul type de ressource, et non **toutes les ressources**, avec cette option.
- L'option **summary** affiche l'utilisation combinée de tous les contextes.
- L'option **system** affiche toutes les utilisations de contexte combinées, mais affiche les limites du système pour les ressources au lieu des limites de contexte combinées.
- Pour la **ressource** *resource_name*, consultez Configurer une classe pour la gestion des ressources, à la page 242 pour connaître les noms de ressources disponibles. Consultez également la commande **show resource type**. Spécifiez **tout** (par défaut) pour tous les types.
- L'option **detail** affiche l'utilisation de toutes les ressources, y compris celles que vous ne pouvez pas gérer. Par exemple, vous pouvez afficher le nombre d'interceptions TCP.
- Le **compteur** *counter_name* est l'un des mots clés suivants :
  - **current** : affiche les instances simultanées actives ou le débit actuel de la ressource.
  - **denied** : affiche le nombre d'instances qui ont été refusées parce qu'elles dépassaient la limite de ressources indiquée dans la colonne Limit (Limite).
  - **max** : affiche le nombre maximum d'instances simultanées ou le débit maximum de la ressource depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage** , soit en raison du redémarrage du périphérique.
  - **all** (par défaut) : affiche toutes les statistiques.
- Le *count_threshold* définit le nombre au-dessus duquel les ressources sont affichées. La valeur par défaut est 1. Si l'utilisation de la ressource est inférieure au nombre que vous avez défini, la ressource n'est pas affichée. Si vous spécifiez **all** pour le nom du compteur, le *count_threshold* s'applique à l'utilisation actuelle.
- Pour afficher toutes les ressources, définissez le *count_threshold* sur **0**.

Exemples

Voici un exemple de sortie de la commande **show resource usage context**, qui affiche l'utilisation des ressources pour le contexte d'administration :

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

Voici un exemple de sortie de la commande **show resource usage summary**, qui affiche l'utilisation des ressources pour tous les contextes et toutes les ressources. Cet exemple montre les limites de six contextes.

```
ciscoasa# show resource usage summary
```

```
Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      N/A            0 Summary
Conns                     584          763      280000(S)      0 Summary
Xlates                   8526         8966      N/A            0 Summary
Hosts                     254          254      N/A            0 Summary
Conns [rate]              270          535      N/A         1704 Summary
Inspects [rate]           270          535      N/A            0 Summary
AnyConnect                  2           25      1000           0 Summary
AnyConnectBurst             0            0      200            0 Summary
Other VPN Sessions          0           10      10           740 Summary
Other VPN Burst             0           10      10           730 Summary

S = System: Combined context limits exceed the system limit; the system limit is shown.
```

Voici un exemple de sortie de la commande **show resource usage summary**, qui affiche les limites pour 25 contextes. Étant donné que la limite de contexte pour les connexions Telnet et SSH est de 5 par contexte, la limite combinée est de 125. La limite du système n'étant que de 100, c'est cette limite qui est affichée.

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

Voici un exemple de sortie de la commande **show resource usage system**, qui affiche l'utilisation des ressources pour tous les contextes, mais qui indique la limite du système au lieu des limites combinées des contextes. L'option **counter all 0** est utilisée pour afficher les ressources qui ne sont pas utilisées actuellement. Les statistiques Denied indiquent le nombre de fois où la ressource a été refusée en raison de la limite du système, si disponible.

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit        Denied    Context
Telnet                      0            0        100             0    System
SSH                         0            0        100             0    System
ASDM                        0            0         32             0    System
Routes                      0            0        N/A             0    System
IPSec                       0            0          5             0    System
Syslogs [rate]              1           18        N/A             0    System
Conns                       0            1     280000             0    System
Xlates                      0            0        N/A             0    System
Hosts                       0            2        N/A             0    System
Conns [rate]                1            1        N/A             0    System
Inspects [rate]             0            0        N/A             0    System
AnyConnect                  2           25      10000             0    System
AnyConnectBurst             0            0        200             0    System
Other VPN Sessions          0           10        750           740    System
Other VPN Burst             0           10        750           730    System
```

Superviser les attaques SYN dans les contextes

L'ASA empêche les attaques SYN à l'aide de l'interception TCP. L'interception TCP utilise l'algorithme des témoins SYN pour empêcher les attaques par inondation TCP SYN. Une attaque par inondation SYN consiste en une série de paquets SYN provenant généralement d'adresses IP falsifiées. Le flux constant de paquets SYN maintient la file d'attente SYN du serveur pleine, ce qui l'empêche de répondre aux demandes de connexion. Lorsque le seuil de connexion amorce d'une connexion est franchi, l'ASA agit comme un serveur mandataire pour le serveur et génère une réponse SYN-ACK à la requête SYN du client. Lorsque l'ASA reçoit un ACK en retour du client, il peut alors authentifier le client et autoriser la connexion au serveur.

Procédure

Étape 1 Supervisez le taux d'attaques pour les contextes individuels :

show perfmon

Étape 2 Supervisez la quantité de ressources utilisées par l'interception TCP pour les contextes individuels :

show resource usage detail

Étape 3 Supervisez les ressources utilisées par l'interception TCP pour l'ensemble du système :

show resource usage summary detail

Exemples

Voici un exemple de sortie de la commande **show perfmon** qui affiche le taux d'interceptions TCP pour un contexte appelé admin.

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept    322779/s      322779/s
```

Voici un exemple de sortie de la commande **show resource usage detail** qui affiche la quantité de ressources utilisées par l'interception TCP pour les contextes individuels. (L'exemple de texte en **gras** affiche les renseignements d'interception TCP.)

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit        Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
chunk:static                1            1  unlimited             0 admin
tcp-intercepts         328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
statics                     1            1  unlimited             0 admin
ace-rules                   1            1  unlimited             0 admin
console-access-rul          2            2  unlimited             0 admin
fixup-rules                14           15  unlimited             0 admin
memory                 959872       960000  unlimited             0 c1
chunk:channels             15           16  unlimited             0 c1
chunk:dbgtrace              1            1  unlimited             0 c1
chunk:fixup                15           15  unlimited             0 c1
chunk:global                1            1  unlimited             0 c1
chunk:hole                  2            2  unlimited             0 c1
chunk:ip-users             10           10  unlimited             0 c1
chunk:udp-ctrl-blk          1            1  unlimited             0 c1
chunk:list-elem            24           24  unlimited             0 c1
chunk:list-hdr              5            6  unlimited             0 c1
chunk:nat                   1            1  unlimited             0 c1
chunk:route                 2            2  unlimited             0 c1
chunk:static                1            1  unlimited             0 c1
tcp-intercept-rate      16056        16254  unlimited             0 c1
globals                     1            1  unlimited             0 c1
np-statics                  3            3  unlimited             0 c1
statics                     1            1  unlimited             0 c1
nats                        1            1  unlimited             0 c1
ace-rules                   2            2  unlimited             0 c1
console-access-rul          2            2  unlimited             0 c1
fixup-rules                14           15  unlimited             0 c1
memory              232695716    232020648  unlimited             0 system
chunk:channels             17           20  unlimited             0 system
chunk:dbgtrace              3            3  unlimited             0 system
chunk:fixup                15           15  unlimited             0 system
chunk:ip-users              4            4  unlimited             0 system
chunk:list-elem          1014         1014  unlimited             0 system
chunk:list-hdr              1            1  unlimited             0 system
chunk:route                 1            1  unlimited             0 system
block:16384               510          885  unlimited             0 system
block:2048                 32           34  unlimited             0 system
```

L'exemple de sortie suivant affiche les ressources utilisées par l'interception TCP pour l'ensemble du système. (L'exemple de texte en **gras** affiche les renseignements d'interception TCP.)

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory              238421312    238434336  unlimited             0 Summary
chunk:channels             46           48  unlimited             0 Summary
chunk:dbgtrace              4            4  unlimited             0 Summary
chunk:fixup                45           45  unlimited             0 Summary
chunk:global                1            1  unlimited             0 Summary
chunk:hole                  3            3  unlimited             0 Summary
chunk:ip-users             24           24  unlimited             0 Summary
```

```
chunk:udp-ctrl-blk          1           1  unlimited            0 Summary
chunk:list-elem          1059        1059  unlimited            0 Summary
chunk:list-hdr             10          11  unlimited            0 Summary
chunk:nat                   1           1  unlimited            0 Summary
chunk:route                 5           5  unlimited            0 Summary
chunk:static                2           2  unlimited            0 Summary
block:16384               510         885  unlimited            0 Summary
block:2048                 32          35  unlimited            0 Summary
tcp-intercept-rate     341306      811579  unlimited            0 Summary
globals                     1           1  unlimited            0 Summary
np-statics                  6           6  unlimited            0 Summary
statics                     2           2        N/A            0 Summary
nats                        1           1        N/A            0 Summary
ace-rules                   3           3        N/A            0 Summary
console-access-rul          4           4        N/A            0 Summary
fixup-rules                43          44        N/A            0 Summary
```

Afficher les adresses MAC attribuées

Vous pouvez afficher les adresses MAC générées automatiquement dans la configuration système ou dans le contexte.

Afficher les adresses MAC dans la configuration système

Cette section décrit comment afficher les adresses MAC dans la configuration système.

Avant de commencer

Si vous attribuez manuellement une adresse MAC à une interface, mais que la génération automatique est également activée, l'adresse générée automatiquement continue de s'afficher dans la configuration même si l'adresse MAC manuelle est celle qui est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement s'affichera.

Procédure

Affichez les adresses MAC attribuées à partir de l'espace d'exécution du système :

show running-config all context [*name*]

L'option **all** (toutes) est requise pour afficher les adresses MAC attribuées. Bien que la commande **mac-address auto** puisse être configurée par l'utilisateur uniquement en mode de configuration globale, la commande s'affiche comme une entrée en lecture seule en mode de configuration du contexte avec l'adresse MAC attribuée. Seules les interfaces allouées qui sont configurées avec une commande **nameif** dans le contexte se voient attribuer une adresse MAC.

Exemples

La sortie suivante de la commande **show running-config all context admin** affiche les adresses MAC principale et de secours attribuées à l'interface de gestion Management0/0 :

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

La sortie suivante de la commande **show running-config all context** affiche toutes les adresses MAC (principales et de secours) pour toutes les interfaces de contexte. Notez que comme les interfaces principales GigabitEthernet0/0 et GigabitEthernet0/1 ne sont pas configurées avec la commande **nameif** dans les contextes, aucune adresse MAC n'a été générée pour elles.

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

Afficher les adresses MAC dans un contexte

Cette section décrit comment afficher les adresses MAC dans un contexte.

Procédure

Affichez l'adresse MAC utilisée par chaque interface dans le contexte :

show interface | include (Interface)|(MAC)

Exemple

Par exemple :

```
ciscoasa/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

Remarque La commande **show interface** affiche l'adresse MAC utilisée; si vous attribuez manuellement une adresse MAC et que la génération automatique est activée, vous ne pouvez afficher que l'adresse générée automatiquement inutilisée à partir de la configuration système.

Exemples de mode de contexte multiple

L'exemple suivant :

- Définit automatiquement les adresses MAC dans les contextes avec un préfixe personnalisé.
- Définit la limite de classe par défaut des connexions à 10 % au lieu d'un nombre illimité et définit le VPN pour les autres sessions à 10, avec une rafale de 5.
- Crée une classe de ressources Gold.
- Définit le contexte d'administration comme « administrateur ».
- Crée un contexte appelé « administrateur » sur la mémoire flash interne pour qu'il fasse partie de la classe de ressources par défaut.
- Ajoute deux contextes d'un serveur FTP dans le cadre de la classe de ressources Gold.

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 10
```

```
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50

ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

Historique du mode de contexte multiple

Tableau 11 : Historique du mode de contexte multiple

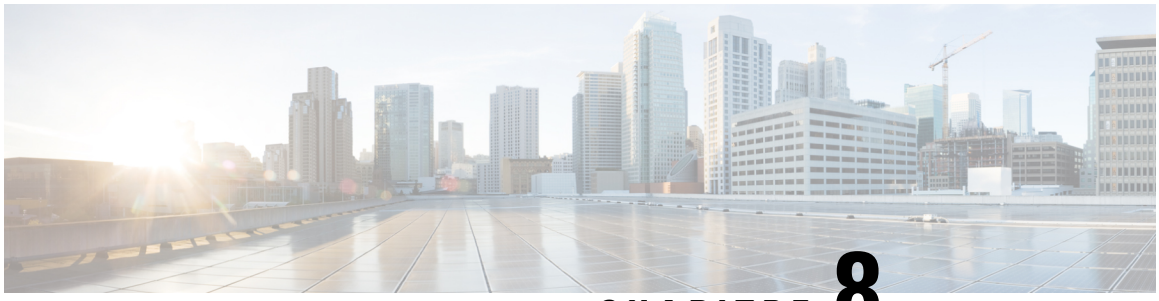
Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Contextes de sécurité multiples	7.0(1)	Le mode de contexte multiple a été introduit. Nous avons introduit les commandes suivantes : **context**, **mode** et **class**.
Affectation automatique de l'adresse MAC	7.2(1)	L'affectation automatique de l'adresse MAC aux interfaces de contexte a été introduite. Nous avons introduit la commande suivante : **mac-address auto**.
Gestion des ressources	7.2(1)	La gestion des ressources a été introduite. Nous avons introduit les commandes suivantes : **class**, **limit-resource** et **member**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Capteurs virtuels pour IPS	8.0(2)	L'AIP SSM exécutant la version 6.0 et ultérieure du logiciel IPS peut exécuter plusieurs capteurs virtuels, ce qui signifie que vous pouvez configurer plusieurs politiques de sécurité sur l'AIP SSM. Vous pouvez affecter chaque contexte ou ASA en mode unique à un ou plusieurs capteurs virtuels, ou vous pouvez attribuer plusieurs contextes de sécurité au même capteur virtuel. Nous avons introduit la commande suivante : **allocate-ips**.
Améliorations de l'affectation automatique de l'adresse MAC	8.0(5)/8.2(2)	Le format de l'adresse MAC a été modifié pour utiliser un préfixe, une valeur initiale fixe (A2) et un schéma différent pour les adresses MAC des unités principale et secondaire dans une paire de basculement. Les adresses MAC sont également conservées de façon permanente pendant les rechargements. L'analyseur de commande vérifie maintenant si la génération automatique est activée; si vous souhaitez également attribuer manuellement une adresse MAC, vous ne pouvez pas commencer l'adresse MAC manuelle par A2. Nous avons modifié la commande suivante : **mac-address auto prefix**.
Augmentation du nombre maximum de contextes pour les modèles ASA 5550 et 5580	v 8.4(1)	Le nombre maximum de contextes de sécurité pour l'ASA 5550 est passé de 50 à 100. Le nombre maximum pour l'ASA 5580 est passé de 50 à 250.
Affectation automatique de l'adresse MAC activée par défaut	8.5(1)	L'affectation automatique de l'adresse MAC est maintenant activée par défaut. Nous avons modifié la commande suivante : **mac-address auto**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Génération automatique d'un préfixe d'adresse MAC	8.6(1)	En mode de contexte multiple, l'ASA convertit maintenant la configuration de génération automatique de l'adresse MAC en utilisant un préfixe par défaut. L'ASA génère automatiquement ce dernier en fonction des deux derniers octets de l'adresse MAC de l'interface (ASA 5500-X) ou du fond de panier (ASASM). Cette conversion se produit automatiquement lorsque vous rechargez ou si vous réactivez la génération d'adresse MAC. La méthode de génération du préfixe offre de nombreux avantages, notamment une meilleure garantie d'adresses MAC uniques sur un segment. Vous pouvez afficher le préfixe généré automatiquement en saisissant la commande **show running-config mac-address**. Si vous souhaitez modifier le préfixe, vous pouvez reconfigurer la fonctionnalité avec un préfixe personnalisé. L'ancienne méthode de génération d'adresse MAC n'est plus disponible. **Remarque** Pour maintenir la mise à niveau sans interruption pour les paires de basculement, l'ASA ne convertit *pas* la méthode de génération d'adresse MAC en une configuration existante lors d'un rechargement si le basculement est activé. Cependant, nous vous conseillons fortement de passer manuellement à la méthode de génération du préfixe lorsque vous utilisez le basculement, en particulier pour l'ASASM. Sans la méthode de préfixe, les ASASM installés dans différents numéros de logement subissent un changement d'adresse MAC lors du basculement et peuvent connaître une interruption du trafic. Après la mise à niveau, pour utiliser la méthode de préfixe de génération d'adresse MAC, réactivez la génération d'adresse MAC pour utiliser le préfixe par défaut. Nous avons modifié la commande suivante : **mac-address auto**.
Affectation automatique de l'adresse MAC désactivée par défaut sur tous les modèles à l'exception de l'ASASM	9.0(1)	L'affectation automatique de l'adresse MAC est maintenant désactivée par défaut, à l'exception de l'ASASM. Nous avons modifié la commande suivante : **mac-address auto**.
Routage dynamique dans les contextes de sécurité	9.0(1)	Les protocoles de routage dynamique EIGRP et OSPFv2 sont désormais pris en charge en mode de contexte multiple. Les routages OSPFv3, RIP et multidiffusion ne sont pas pris en charge.
Nouveau type de ressource pour les entrées de la table de routage	9.0(1)	Un nouveau type de ressource, les routes, a été créé pour définir le nombre maximum d'entrées de table de routage dans chaque contexte. Nous avons modifié les commandes suivantes : **limit-resource, show resource types, show resource usage, show resource allocation**.
VPN de site à site en mode de contexte multiple	9.0(1)	Les tunnels VPN de site à site sont désormais pris en charge en mode de contexte multiple.
Nouveau type de ressource pour les tunnels VPN de site à site	9.0(1)	De nouveaux types de ressources (vpn other et vpn burst other) ont été créés pour définir le nombre maximum de tunnels VPN de site à site dans chaque contexte. Nous avons modifié les commandes suivantes : **limit-resource, show resource types, show resource usage, show resource allocation**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Nouveau type de ressource pour les négociations de la SA IKEv1	9.1(2)	Un nouveau type de ressource (ikev1 in-negotiation) a été créé pour définir le pourcentage maximum de négociations de la SA IKEv1 dans chaque contexte afin d'éviter de submerger le CPU et les moteurs de chiffrement. Sous certaines conditions (certificats volumineux, vérification des CRL), vous souhaiterez peut-être restreindre cette ressource. Nous avons modifié les commandes suivantes : **limit-resource, show resource types, show resource usage, show resource allocation**.
Prise en charge du VPN d'accès à distance en mode de contexte multiple	9.5(2)	Vous pouvez désormais utiliser les fonctionnalités d'accès à distance suivantes en mode de contexte multiple : • AnyConnect 3.x ou versions ultérieures (SSL VPN uniquement; pas de prise en charge d'IKEv2) • Configuration centralisée de l'image Secure Client (services client sécurisés) • Mise à niveau de l'image Secure Client (services client sécurisés) • Gestion des ressources de contexte pour les connexions Secure Client (services client sécurisés) **Remarque** La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante. Nous avons introduit les commandes suivantes : **limit-resource vpn anyconnect, limit-resource vpn burst anyconnect**
Fonction de préremplissage/nom d'utilisateur à partir du certificat pour le mode de contexte multiple	9.6(2)	La prise en charge de SSL Secure Client (services client sécurisés) est étendue, ce qui permet aux interfaces de ligne de commande de la fonctionnalité de préremplissage/nom d'utilisateur à partir du certificat, qui étaient auparavant seulement disponibles en mode unique, d'être également activées en mode de contexte multiple. Nous n'avons pas modifié de commandes.
Virtualisation flash pour le VPN d'accès à distance	9.6(2)	Le VPN d'accès à distance en mode de contexte multiple prend désormais en charge la virtualisation flash. Chaque contexte peut avoir un espace de stockage privé et un emplacement de stockage partagé en fonction de la mémoire flash totale disponible : • Stockage privé : stockez les fichiers associés uniquement à cet utilisateur et spécifiques au contenu que vous souhaitez pour cet utilisateur. • Stockage partagé : chargez des fichiers dans cet espace et rendez-le accessible à n'importe quel contexte d'utilisateur pour un accès en lecture/écriture une fois que vous l'avez activé. Nous avons introduit les commandes suivantes : **limit-resource storage, storage-url**
Profils Secure Client (services client sécurisés) pris en charge dans les périphériques en contexte multiple	9.6(2)	Les profils Secure Client (services client sécurisés) sont pris en charge dans les périphériques en contexte multiple. Pour ajouter un nouveau profil à l'aide d'ASDM, vous devez disposer de la version Secure Client (services client sécurisés) 4.2.00748 ou 4.3.03013 et ultérieure.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Basculement avec état pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple	9.6(2)	Le basculement avec état est maintenant pris en charge pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple. Nous n'avons pas modifié de commandes.
La politique d'accès dynamique (DAP) du VPN d'accès à distance est prise en charge en mode de contexte multiple	9.6(2)	Vous pouvez maintenant configurer la DAP par contexte en mode de contexte multiple. Nous n'avons pas modifié de commandes.
Le CoA (changement d'autorisation) du VPN d'accès à distance est pris en charge en mode de contexte multiple	9.6(2)	Vous pouvez maintenant configurer le CoA par contexte en mode de contexte multiple. Nous n'avons pas modifié de commandes.
La localisation du VPN d'accès à distance est prise en charge en mode de contexte multiple	9.6(2)	La localisation est prise en charge dans le monde entier. Il n'y a qu'un seul ensemble de fichiers de localisation partagés dans différents contextes. Nous n'avons pas modifié de commandes.
Le VPN d'accès à distance pour IKEv2 est pris en charge en mode de contexte multiple	9.9(2)	Vous pouvez configurer le VPN d'accès à distance en mode de contexte multiple pour IKEv2.
Limitation configurable des sessions d'administration	9.12(1)	Vous pouvez configurer le nombre maximum de sessions administratives agrégées, par utilisateur et par protocole. Auparavant, vous pouviez configurer uniquement le nombre agrégé de sessions. Cette fonctionnalité n'influe pas sur les sessions de console. Notez qu'en mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions HTTPS, où le maximum est fixé à 5 sessions. La commande **quota management-session** n'est également plus acceptée dans la configuration système et est plutôt disponible dans la configuration du contexte. Le nombre maximum de sessions agrégées est désormais de 15; si vous avez configuré 0 (illimité) ou 16+, lors de la mise à niveau, la valeur passe à 15. Commandes nouvelles/modifiées : **quota management-session**, **show quota management-session**
Le nombre maximum de contextes de Firepower 1140 est passé de 5 à 10	9.16(1)	Le Firepower 1140 prend désormais en charge jusqu'à 10 contextes.



CHAPITRE 8

Basculement pour la haute disponibilité

Ce chapitre décrit comment configurer le basculement actif/en attente ou actif/actif pour une haute disponibilité de l'ASA.

- À propos du basculement, à la page 273
- Licences pour le basculement, à la page 295
- Lignes directrices pour Failover (basculement), à la page 296
- Paramètres par défaut pour le basculement, à la page 299
- Configurer le basculement actif/de secours, à la page 299
- Configurer le basculement actif/actif, à la page 304
- Configurer les paramètres de basculement facultatifs, à la page 310
- Gérer Failover (basculement), à la page 319
- Surveillance de Failover (basculement), à la page 325
- Historique de basculement, à la page 326

À propos du basculement

La configuration du basculement nécessite deux ASA identiques connectés l'un à l'autre par une liaison de basculement dédiée et, éventuellement, un lien d'état. L'intégrité des unités actives et des interfaces est supervisée pour déterminer si elles répondent aux conditions de basculement spécifiques. Si ces conditions sont remplies, le basculement se produit.

Modes de basculement

L'ASA prend en charge deux modes de basculement : le basculement actif/actif et le basculement actif/veille. Chaque mode de basculement a sa propre méthode pour déterminer et effectuer le basculement.

- Dans le basculement actif/veille, un périphérique agit en tant qu'unité active et achemine le trafic. Le deuxième périphérique, désigné comme unité de veille, ne transmet pas activement le trafic. Lors d'un basculement, l'unité active est remplacée par l'unité de veille, qui devient alors active. Vous pouvez utiliser le basculement actif/veille pour les ASA en mode de contexte unique ou multiple.
- Dans une configuration de basculement actif/actif, les deux ASA peuvent transmettre le trafic réseau. Le basculement actif/actif n'est disponible que pour les ASA en mode de contexte multiple. Dans le basculement actif/actif, vous divisez les contextes de sécurité sur l'ASA en 2 *groupes de basculement*. Un groupe de basculement est simplement un groupe logique d'un ou plusieurs contextes de sécurité.

Un groupe est attribué pour être actif sur l'ASA principal, et l'autre groupe est attribué pour être actif sur l'ASA secondaire. Lorsqu'un basculement se produit, il se produit au niveau du groupe de basculement.

Les deux modes de basculement prennent en charge le basculement avec ou sans état.

Configuration système requise pour Failover (basculement)

Cette section décrit les exigences matérielles, logicielles et de licence pour les périphériques ASA dans une configuration Failover (basculement).

Configuration matérielle requise

Les deux unités dans une configuration Failover (basculement) doivent :

- être du même modèle.

  Pour la Firepower 9300, la haute disponibilité est uniquement prise en charge entre les modules de même type; toutefois, les deux châssis peuvent inclure des modules mixtes. Par exemple, chaque châssis a un SM-56, SM-48 et SM-40. Vous pouvez créer des paires à haute accessibilité entre les modules SM-56, entre les modules SM-48 et entre les modules SM-40.

- Avoir le même nombre et les mêmes types d'interfaces.

  Pour le Firepower 2100 en mode Plateforme et Châssis Firepower 4100/9300 , toutes les interfaces doivent être préconfigurées en FXOS de manière identique avant d'activer Failover (basculement). Si vous modifiez les interfaces après avoir activé Failover (basculement), modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active. Si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation ASA.

- Ayez les mêmes modules installés (le cas échéant);

- Ayez la même RAM installée.

Si vous utilisez des unités avec des tailles de mémoire flash différentes dans votre configuration Failover (basculement), assurez-vous que l'unité dotée de la mémoire flash la plus faible dispose de suffisamment d'espace pour contenir les fichiers d'image logicielle et les fichiers de configuration. Si ce n'est pas le cas, la synchronisation de la configuration de l'unité ayant la plus grande mémoire flash vers l'unité ayant la plus faible mémoire flash échouera.

Configuration logicielle requise

Les deux unités dans une configuration Failover (basculement) doivent :

- Être dans le même mode de contexte (simple ou multiple).

- Pour le mode unique : utilisez le même mode de pare-feu (routage ou transparent).

  Dans le mode de contexte multiple, le mode de pare-feu est défini au niveau du contexte et vous pouvez utiliser des modes mixtes.

- Avoir les mêmes version majeure (premier numéro) et mineure (deuxième numéro). Cependant, vous pouvez utiliser temporairement différentes versions du logiciel au cours d'un processus de mise à niveau. Par exemple, vous pouvez mettre à niveau une unité de la version 8.3(1) à la version 8.3(2) et faire en sorte que le basculement reste actif. Nous vous recommandons de mettre à niveau les deux unités à la même version pour assurer la compatibilité à long terme.
- Avoir les mêmes images Secure Client (services client sécurisés). Si les images de la paire de basculement ne concordent pas lorsqu'une mise à niveau sans appel est effectuée, la connexion du VPN SSL sans client s'interrompt à l'étape de redémarrage final du processus de mise à niveau, la base de données affiche une session orpheline et l'ensemble d'adresses IP indique que l'adresse IP attribuée au le client est « en cours d'utilisation ».
- Être dans le même mode FIPS.
- (Firepower 4100/9300) ont le même mode de déchargement de flux, activé ou désactivé.

Exigences de licence

Il n'est pas nécessaire que les deux unités d'une configuration de basculement aient des licences identiques; les licences se combinent pour créer une licence de grappe de basculement.

Liens de basculement et de basculement avec état

Le lien de basculement et le lien de basculement dynamique facultatif sont des connexions dédiées entre les deux unités. Cisco recommande d'utiliser la même interface entre deux périphériques dans une liaison de basculement ou un lien de basculement avec état. Par exemple, dans un lien de basculement, si vous avez utilisé eth0 dans le périphérique 1, utilisez également la même interface (eth0) dans le périphérique 2.



Mise en garde Toutes les informations envoyées sur les liens de basculement et d'état sont envoyées en texte clair, sauf si vous sécurisez la communication avec un tunnel IPsec ou une clé de basculement. Si l'ASA est utilisé pour mettre fin à des tunnels VPN, cette information comprend les noms d'utilisateur, les mots de passe et les clés prépartagées utilisés pour l'établissement des tunnels. La transmission de ces données sensibles en texte clair peut présenter un risque de sécurité important. Nous vous recommandons de sécuriser la communication de basculement avec un tunnel IPsec ou une clé de basculement si vous utilisez l'ASA pour mettre fin aux tunnels VPN.

Lien de basculement

Les deux unités d'une paire de basculement communiquent en permanence sur une liaison de basculement pour déterminer l'état de fonctionnement de chaque unité.

Données de la liaison de basculement

Les informations suivantes sont transmises par la liaison de basculement :

- L'état de l'unité (actif ou en veille)
- Messages Hello (keep-alives)
- État de la liaison réseau
- Échange d'adresses MAC

- Réplication et synchronisation de la configuration

Interface de la liaison de basculement

Vous pouvez utiliser une interface de données inutilisée (physique, sous-interface ou EtherChannel) comme liaison de basculement; cependant, vous ne pouvez pas spécifier une interface actuellement configurée avec un nom. L'interface de liaison de basculement n'est pas configurée comme une interface réseau normale; il existe pour la communication de basculement uniquement. Cette interface ne peut être utilisée que pour la liaison de basculement (ainsi que pour le lien d'état). Pour la plupart des modèles, vous ne pouvez pas utiliser une interface de gestion pour le basculement, à moins que cela ne soit explicitement décrit ci-dessous.

Le ASA ne prend pas en charge les interfaces de partage entre les données de l'utilisateur et le lien de basculement. Vous ne pouvez pas non plus utiliser des sous-interfaces distinctes sur le même parent pour la liaison de basculement et pour les données.

Consultez les consignes suivantes concernant la liaison de basculement :

- 5506-X à 5555-X : vous ne pouvez pas utiliser l'interface de gestion comme liaison de basculement; vous devez utiliser une interface de données. La seule exception est pour le modèle 5506H-X, où vous pouvez utiliser l'interface de gestion comme liaison de basculement.
- 5506H-X : vous *pouvez* utiliser l'interface de gestion Management 1/1 comme liaison de basculement. Si vous le configurez pour le basculement, vous devez recharger le périphérique pour que la modification prenne effet. Dans ce cas, vous ne pouvez pas également utiliser le module ASA Firepower, car il nécessite l'interface de gestion à des fins de gestion.
- Firepower 4100/9300 : vous ne pouvez pas utiliser l'interface de type de gestion pour la liaison de basculement.
- Consultez les lignes directrices suivantes pour dimensionner la liaison.

Tableau 12 : Taille de la liaison de basculement

Modèle	Taille de l'interface pour la liaison combinée de basculement et d'état
Firepower 1010	1 Gbit/sec
Firepower 1100	1 Gbit/sec
Firepower de la série 2100	1 Gbit/sec
Secure Firewall 3100	Secure Firewall 3105, 1 Gbit/s Secure Firewall 3110, 1 Gbit/s Secure Firewall 3120, 1 Gbit/s Secure Firewall 3130, 10 Gbit/s Secure Firewall 3140, 10 Gbit/s
Firepower 4100	10 Gbit/s
Firepower 9300	10 Gbit/s

La fréquence d'alternance est égale au temps de maintien de l'unité (la commande **failover polltime unit**).

Remarque Si vous avez une configuration importante et un temps d'attente d'unité faible, l'alternance entre les interfaces membres peut empêcher l'unité secondaire de se joindre ou de se joindre. Dans ce cas, désactivez l'une des interfaces membres jusqu'à ce que l'unité secondaire se soit jointe.

Pour un EtherChannel utilisé comme liaison de basculement, pour éviter les paquets dans le désordre, une seule interface dans l'EtherChannel est utilisée. Si cette interface échoue, l'interface suivante de l'EtherChannel est utilisée. Vous ne pouvez pas modifier la configuration de l'EtherChannel lorsqu'il est utilisé comme liaison de basculement.

Connexion de la liaison de basculement

Connectez le lien de basculement de l'une des deux manières suivantes :

- À l'aide d'un commutateur, sans autre périphérique sur le même segment de réseau (domaine de diffusion ou VLAN) que les interfaces de basculement du ASA Firewall Threat Defense.
- L'utilisation d'un câble Ethernet pour connecter les unités directement, sans avoir besoin d'un commutateur externe.

Si vous n'utilisez pas de commutateur entre les unités, et en cas de défaillance de l'interface, la liaison est interrompue sur les deux homologues. Cette condition peut nuire aux efforts de dépannage, car vous ne pouvez pas facilement déterminer quelle unité a l'interface défaillante qui a entraîné la défaillance du lien.

LeASA Firewall Threat Defense prend en charge Auto-MDI/MDIX sur ses ports Ethernet en cuivre, vous pouvez donc utiliser un câble croisé ou droit. Si vous utilisez un câble droit, l'interface détecte automatiquement le câble et échange l'une des paires de transmission/réception contre MDIX.

Lien de basculement dynamique

Pour utiliser le basculement avec état, vous devez configurer un lien de basculement avec état (également appelé lien d'état) pour transmettre les informations sur l'état de la connexion.

Partagé avec la liaison de basculement

Le partage d'un lien de basculement est le meilleur moyen de conserver les interfaces. Cependant, vous devez envisager une interface dédiée pour le lien d'état et le lien de basculement, si votre configuration est importante et que le trafic sur le réseau est élevé.

Interface dédiée

Vous pouvez utiliser une interface de données dédiée (physique ou EtherChannel) pour la liaison d'état. Consultez Interface de la liaison de basculement, à la page 276 pour connaître les exigences relatives à une lien liaison d'état dédiée et Connexion de la liaison de basculement, à la page 277 pour obtenir des renseignements sur la façon de connecter la liaison d'état.

Pour des performances optimales lors de l'utilisation du basculement longue distance, la latence de la liaison d'état doit être inférieure à 10 millisecondes et non supérieure à 250 millisecondes. Si la latence est supérieure à 10 millisecondes, une certaine dégradation des performances se produit en raison de la retransmission des messages de basculement.

Éviter le basculement interrompu et les liaisons de données

Nous recommandons que les liens de basculement et les interfaces de données empruntent différentes voies pour réduire le risque d'échec de toutes les interfaces en même temps. Si la liaison de basculement est hors service, l'ASA peut utiliser les interfaces de données pour déterminer si un basculement est requis. Ensuite, l'opération de basculement est suspendue jusqu'à ce que l'intégrité du lien de basculement soit restaurée.

Consultez les scénarios de connexion suivants pour concevoir un réseau de basculement résilient.

Scénario 1 (non recommandé)

Si un seul commutateur ou un ensemble de commutateurs est utilisé pour connecter les interfaces de basculement et de données entre deux ASA, quand un commutateur ou une liaison inter-commutateurs sont en panne, les deux ASA deviennent actifs. Par conséquent, les deux méthodes de connexion illustrées dans les figures suivantes ne sont PAS conseillées.

Illustration 43 : Connexion avec un commutateur unique : non recommandée

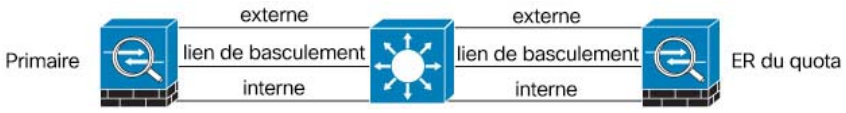


Illustration 44 : Connexion avec un double commutateur : non recommandée



Scénario 2 (recommandé)

Nous conseillons que les liaisons de basculement n'utilisent PAS le même commutateur que les interfaces de données. Au lieu de cela, utilisez un commutateur différent ou utilisez un câble direct pour connecter le lien de basculement, comme le montrent les figures suivantes.

Illustration 45 : Connexion avec un autre commutateur

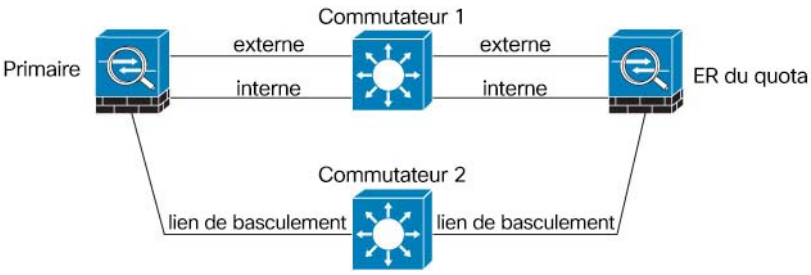
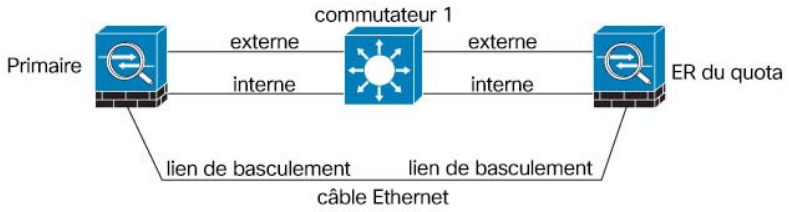


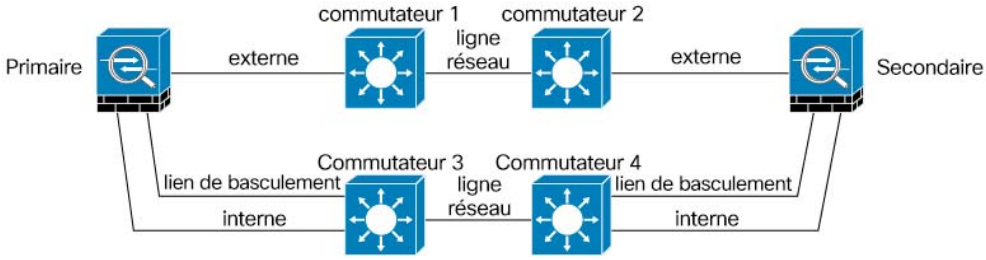
Illustration 46 : Connexion avec un câble



Scénario 3 (recommandé)

Si les interfaces de données ASA sont connectées à plusieurs ensembles de commutateurs, un lien de basculement peut être connecté à l'un des commutateurs, de préférence le commutateur du côté sécurisé (interne) du réseau, comme le montre la figure suivante.

Illustration 47 : Connexion avec un commutateur sécurisé



Les adresses MAC et les adresses IP en Failover (basculement)

Lorsque vous configurez vos interfaces, vous pouvez spécifier une adresse IP active et une adresse IP de secours sur le même réseau. En général, lors d'un basculement, la nouvelle unité active prend en charge les adresses IP et MAC actives. Étant donné que les périphériques réseau ne constatent aucun changement dans l'association d'adresses MAC à l'adresse IP, aucune entrée ARP ne change et n'expire sur le réseau.

Remarque Bien que recommandée, l'adresse de secours n'est pas obligatoire. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien. Vous ne pouvez pas non plus vous connecter à l'unité de secours sur cette interface à des fins de gestion.

L'adresse IP et l'adresse MAC du lien d'état ne changent pas lors du basculement.

Adresses IP et adresses MAC actives/en attente

Pour le Failover (basculement) (actif/veille), consultez les documents suivants pour connaître l'utilisation de l'adresse IP et de l'adresse MAC lors d'un événement de basculement :

1. L'unité active utilise toujours les adresses IP et MAC de l'unité principale.
2. Lorsque l'unité active bascule, l'unité en veille adopte les adresses IP et MAC de l'unité défaillante et commence à transmettre le trafic.

3. Lorsque l'unité défaillante est remise en ligne, elle est maintenant en état de veille et prend le relais des adresses IP et MAC de secours.

Toutefois, si l'unité secondaire démarre sans détecter l'unité principale, l'unité secondaire devient l'unité active et utilise ses propres adresses MAC, car elle ne connaît pas les adresses MAC de l'unité principale. Lorsque l'unité principale devient disponible, les adresses MAC de l'unité secondaire (active) changent pour celles de l'unité principale, ce qui peut entraîner une interruption de votre trafic réseau. De même, si vous remplacez l'unité principale par un nouveau matériel, une nouvelle adresse MAC est utilisée.

Si vous désactivez le basculement et définissez les configurations de basculement à un état désactivé, vous devrez reprendre manuellement le basculement ou redémarrer le périphérique. Il est conseillé d'utiliser la commande **failover reset** et de reprendre le basculement au lieu de redémarrer le périphérique. Si vous rechargez l'unité de secours avec la configuration de basculement désactivée, l'unité de secours démarre en tant qu'unité active et utilise les adresses IP et MAC de l'unité principale. Cela conduit à des adresses IP en double et entraîne des perturbations du trafic réseau. Utilisez la commande **failover reset** pour activer le basculement et restaurer le flux de trafic.



Remarque Si vous activez le basculement sur un périphérique autonome, les interfaces de données tombent en panne lors de la négociation du basculement, interrompant le trafic.

Les adresses MAC virtuelles empêchent cette perturbation, car les adresses MAC actives sont connues de l'unité secondaire au démarrage et restent les mêmes dans le cas du nouveau matériel de l'unité principale. Nous vous recommandons de configurer l'adresse MAC virtuelle sur les unités principale et secondaire pour vous assurer que l'unité secondaire utilise les adresses MAC correctes lorsqu'il s'agit de l'unité active, même si elle est mise en ligne avant l'unité principale. Si vous ne configurez pas d'adresses MAC virtuelles, vous devrez peut-être effacer les tableaux ARP sur les routeurs connectés pour restaurer le flux de trafic. ASA n'envoie pas d'ARP gratuits pour les adresses NAT statiques lorsque l'adresse MAC change, de sorte que les routeurs connectés n'apprennent pas le changement d'adresse MAC pour ces adresses.

Adresses IP et adresses MAC actives/actives

Pour le basculement actif, consultez les documents suivants pour connaître l'utilisation de l'adresse IP et de l'adresse MAC lors d'un événement de basculement :

1. L'unité principale génère automatiquement des adresses MAC actives et de secours pour toutes les interfaces dans les contextes des groupes de basculement 1 et 2. Vous pouvez également configurer manuellement les adresses MAC au besoin, par exemple en cas de conflit d'adresses MAC.
2. Chaque unité utilise les adresses IP et MAC actives pour son groupe de basculement actif et les adresses de secours pour son groupe de basculement en veille. Par exemple, l'unité principale est active pour le groupe de basculement 1, elle utilise donc les adresses actives pour les contextes du groupe de basculement 1. Elle est en veille pour les contextes du groupe de basculement 2, où elle utilise les adresses de secours.
3. Lors du basculement d'une unité, l'autre unité prend les adresses IP et les adresses MAC actives du groupe de basculement et commence à transmettre le trafic.
4. Lorsque l'unité défaillante est remise en ligne et que vous avez activé l'option de préemption, elle reprend le groupe de basculement.

Adresses MAC virtuelles

L'ASA comporte plusieurs méthodes pour configurer les adresses MAC virtuelles. Nous vous recommandons d'utiliser une seule méthode. Si vous définissez l'adresse MAC à l'aide de plusieurs méthodes, l'adresse MAC utilisée dépend de nombreuses variables et peut ne pas être prédictible. Les méthodes manuelles comprennent la commande interface mode **mac-address**, la commande **failover mac address** et, pour le basculement actif/actif, la commande failover group mode **mac address**, en plus des méthodes de génération automatique décrites ci-dessous.

En mode de contexte multiple, vous pouvez configurer l'ASA pour générer automatiquement des adresses MAC virtuelles actives et de secours pour les interfaces partagées, et ces affectations sont synchronisées avec l'unité secondaire (voir la commande **mac-address auto**). Pour les interfaces non partagées, vous pouvez définir manuellement les adresses MAC pour le mode actif/veille (le mode actif/actif génère automatiquement les adresses MAC pour toutes les interfaces).

Pour le basculement actif, les adresses MAC virtuelles sont toujours utilisées, avec des valeurs par défaut ou des valeurs que vous pouvez définir par interface.

Mise à jour du tableau d'adresses MAC dans le basculement

Pendant le basculement, le périphérique désigné comme le nouveau périphérique actif génère des paquets de multidiffusion pour chaque entrée d'adresse MAC dans le tableau MAC et les envoie à toutes les interfaces du groupe de ponts. Cette action incite les commutateurs en amont du groupe de ponts à mettre à jour leurs tables de routage avec l'interface du nouveau périphérique actif pour assurer un transfert précis du trafic.

Le temps nécessaire pour générer des paquets de multidiffusion et mettre à jour les tables de routage des commutateurs en amont dépend du nombre d'entrées dans le tableau d'adresses MAC et du nombre d'interfaces du groupe de ponts. Utilisez la commande **show failover statistics state-switch-delay** pour afficher les statistiques relatives aux retards rencontrés lors des événements de basculement.

Basculement avec et sans état

L'ASA prend en charge deux types de basculement, sans état et avec état, pour les modes actif/veille et actif/actif.

Remarque Certains éléments de configuration pour le SSL VPN sans client (comme les signets et la personnalisation) utilisent le sous-système de basculement VPN, qui fait partie du basculement dynamique. Vous devez utiliser le basculement dynamique pour synchroniser ces éléments entre les membres de la paire de basculement. Le basculement sans état n'est pas conseillé pour le SSL VPN sans client.

Basculement sans état

Lorsqu'un basculement se produit, toutes les connexions actives sont abandonnées. Les clients doivent rétablir les connexions lorsque la nouvelle unité active prend le relais.

Remarque Certains éléments de configuration pour le SSL VPN sans client (comme les signets et la personnalisation) utilisent le sous-système de basculement VPN, qui fait partie du basculement dynamique. Vous devez utiliser le basculement dynamique pour synchroniser ces éléments entre les membres de la paire de basculement. Le basculement sans état (standard) n'est pas conseillé pour le SSL VPN sans client.

Basculement avec état

Lorsque le basculement dynamique est activé , l'unité active transmet en permanence des informations sur l'état de la connexion à l'unité en veille, ou en cas de basculement actif/actif, entre les groupes de basculement actif et de secours. Après un basculement, les mêmes informations de connexion sont disponibles sur la nouvelle unité active. Les applications de l'utilisateur final prises en charge ne sont pas tenues de se reconnecter pour conserver la même session de communication.

Fonctionnalités prises en charge

Pour le basculement avec état, les renseignements d'état suivants sont transmis à l'ASA de secours :

- table de traduction NAT
- Les connexions et les états TCP et UDP. Les autres types de protocoles IP et ICMP ne sont pas analysés par l'unité active, car ils sont établis sur la nouvelle unité active à l'arrivée d'un nouveau paquet.
- Le tableau de connexion HTTP (sauf si vous activez la duplication HTTP).
- Les états de la connexion HTTP (si la duplication HTTP est activée) : Par défaut, l'ASA ne reproduit pas les informations de session HTTP lorsque le basculement avec état est activé. Nous vous suggérons d'activer la duplication HTTP.
- États de la connexion SCTP Cependant, le basculement avec état de l'inspection SCTP est préférable. Pendant le basculement, si des paquets SACK sont perdus, la nouvelle unité active abandonnera tous les autres paquets dans le désordre dans la file d'attente jusqu'à ce que le paquet manquant soit reçu.
- La table ARP
- La table des ponts de couche 2 (pour les groupes de ponts)
- La table ISAKMP et IPsec SA
- La base de données sur les connexions GTP-PDP
- Sessions de signalisation SIP et trous d'épingle.
- ICMP connection state (état de connexion ICMP) : la duplication de connexion ICMP n'est activée que si l'interface respective est affectée à un groupe de routage dissymétrique.
- Tables de routage statiques et dynamiques : le basculement dynamique participe aux protocoles de routage dynamiques, tels que OSPF et EIGRP, de sorte que les itinéraires appris par les protocoles de routage dynamiques sur l'unité active sont conservés dans une table RIB (Routing Information Base) sur l'unité en attente. Lors d'un basculement, les paquets se déplacent normalement avec une perturbation minimale du trafic, car l'unité secondaire active est initialement soumise à des règles qui reflètent l'unité principale. Immédiatement après le basculement, le délai de reconvergence démarre sur l'unité nouvellement active. Ensuite, le numéro de la période pour la table RIB est incrémenté. Pendant la reconvergence, les routes OSPF et EIGRP sont mises à jour avec un nouveau numéro de période. Une fois la minuterie expirée, les entrées de route périmées (déterminées par le numéro de période) sont supprimées du tableau. Le RIB contient ensuite les informations de transfert les plus récentes du protocole de routage sur la nouvelle unité active.

Remarque Les routages ne sont synchronisés que pour les événements de connexion ou de déconnexion sur une unité active. Si le lien est actif ou inactif sur l'unité de secours, les routages dynamiques envoyés à partir de l'unité active peuvent être perdus. Ce comportement est tout à fait normal et attendu.

- Serveur DHCP : les baux d'adresses DHCP ne sont pas répliqués. Cependant, un serveur DHCP configuré sur une interface enverra un message ping pour s'assurer qu'une adresse n'est pas utilisée avant d'accorder l'adresse à un client DHCP, donc il n'y a pas d'incidence sur le service. Les informations d'état ne sont pas pertinentes pour le relais DHCP ou DDNS.
- Sessions Cisco IPSoftPhone : Si un basculement se produit pendant une session Cisco IPSoftPhone active, l'appel reste actif, car les informations sur l'état de la session d'appel sont répliquées sur l'unité de secours. Lorsque l'appel est terminé, le client IPSoftPhone perd la connexion avec Cisco Call Manager. Cette perte de connexion se produit parce qu'il n'y a pas d'informations de session pour le message de raccrochage CTIQBE sur l'unité de secours. Lorsque le client IP SoftPhone ne reçoit pas de réponse du gestionnaire d'appels dans un certain délai, il considère que le gestionnaire d'appels est injoignable et se désenregistre.
- VPN d'accès à distance : les utilisateurs finaux du VPN d'accès à distance n'ont pas à s'authentifier ou à reconnecter la session VPN après un basculement. Cependant, les applications fonctionnant sur la connexion VPN pourraient perdre des paquets pendant le processus de basculement et ne pas se rétablir après la perte de paquets.
- De toutes les connexions, seules celles établies seront répliquées sur le périphérique de secours.

Fonctionnalités non prises en charge

Pour le basculement avec état, les informations d'état suivantes ne sont pas transmises au ASA de secours :

- Le tableau d'authentification des utilisateurs (uauth)
- Les connexions de contournement d'état TCP
- Le routage de multidiffusion
- Fonctionnalités sélectionnées du VPN SSL sans client :
  - Tunnels intelligents
  - Transfert de port
  - Modules d'extension
  - Applets Java
  - Sessions IPv6 sans client ou Secure Client (services client sécurisés)
  - Authentification Citrix (les utilisateurs de Citrix doivent se réauthentifier après le basculement)

Exigences en matière de groupes de ponts pour le basculement

Il y a des considérations particulières à prendre en matière de basculement lors de l'utilisation de groupes de ponts.

Exigences en matière de groupes de ponts pour les appareils, ASAv

Lorsque l'unité active bascule sur l'unité en veille, le port du commutateur connecté exécutant le protocole Spanning Tree (STP) peut passer dans un état bloquant pendant 30 à 50 secondes lorsqu'il détecte le changement de topologie. Pour éviter les pertes de trafic lorsque le port est dans un état bloquant, vous pouvez configurer l'une des solutions de contournement suivantes en fonction du mode du port du commutateur :

- Mode d'accès : activez la fonctionnalité STP PortFast sur le commutateur :

  ```
  interface interface_id
    spanning-tree portfast
  ```

  La fonctionnalité PortFast fait immédiatement passer le port en mode de transfert STP lors de l'établissement de la liaison. Le port participe toujours à STP. Ainsi, si le port doit faire partie de la boucle, le port finit par passer en mode de blocage STP.

- Mode de liaison : bloquez les BPDU sur l'ASA sur les interfaces membres d'un groupe de ponts avec un critère d'accès EtherType.

  ```
  access-list id ethertype deny bpdu
  access-group id in interface name1
  access-group id in interface name2
  ```

  Le blocage des BPDU désactive le STP sur le commutateur. Assurez-vous de ne pas avoir de boucles concernant l'ASA dans la disposition de votre réseau.

Si aucune des options ci-dessus n'est possible, vous pouvez utiliser l'une des solutions de contournement moins souhaitables suivantes qui a une incidence sur la fonctionnalité de basculement ou la stabilité STP :

- Désactivez la supervision d'interface.
- Augmentez le temps de rétention à une valeur élevée qui permettra au STP de converger avant le basculement des ASA.
- Réduisez les minuteries STP pour permettre au STP de converger plus rapidement que le temps de rétention de l'interface.

Surveillance de l'intégrité du basculement

Le ASA surveille l'intégrité générale et l'intégrité de l'interface de chaque unité. Cette section comprend des informations sur la façon dont leASA effectue les tests pour déterminer l'état de chaque unité.

Surveillance de l'intégrité de l'unité

Le ASA détermine l'intégrité de l'autre unité en surveillant le lien de basculement à l'aide de messages Hello. Lorsqu'une unité ne reçoit pas trois messages Hello consécutifs sur la liaison de basculement, l'unité envoie des messages LANTEST sur chaque interface de données, y compris la liaison de basculement, pour valider

si l'homologue réagit ou non. Pour les périphériques Firepower 9300 et 4100, vous pouvez activer la surveillance de la détection de transfert bidirectionnel (BFD), qui est plus fiable que les messages Hello. L'action du ASA dépend de la réponse de l'autre unité. Consultez les exemples d'actions suivantes :

- Si le ASA reçoit une réponse sur le lien de basculement, il ne bascule pas.
- Si le ASA ne reçoit pas de réponse sur la liaison de basculement, mais qu'il reçoit une réponse sur une interface de données, l'unité ne bascule pas. Le lien de basculement est marqué comme ayant échoué. Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer sur l'unité de secours lorsque le lien de basculement est inactif.
- Si le ASA ne reçoit de réponse sur aucune interface, l'unité en veille passe en mode actif et classe l'autre unité comme en panne.

Surveillance d'interfaces

Vous pouvez surveiller jusqu'à 1 025 interfaces (en mode contextes multiples, réparties entre tous les contextes). Vous devez surveiller les interfaces importantes. Par exemple, en mode de contexte multiple, vous pouvez configurer un contexte pour surveiller une interface partagée : comme l'interface est partagée, tous les contextes bénéficient de la surveillance.

Lorsqu'une unité ne reçoit pas de messages Hello sur une interface surveillée pendant 15 secondes (valeur par défaut), elle exécute des tests d'interface. (Pour modifier la période, consultez la commande **failover polltime interface** ou, pour le basculement actif/actif, la commande **polltime interface**, (Configuration > Gestion du périphérique > Haute disponibilité et évolutivité > Basculement > Critères > Durées d'interrogation du basculement).) Si l'un des tests d'interface échoue pour une interface, mais que cette même interface sur l'autre unité continue de transmettre le trafic avec succès, l'interface est considérée comme ayant échoué et leASA arrête d'exécuter les tests.

Si le seuil que vous avez défini pour le nombre d'interfaces défaillantes est atteint (voir la commande **failover interface-policy**, ou pour le basculement actif/actif, la commande **interface-policy**) et que l'unité active a plus d'interfaces défaillantes que l'unité en attente, un basculement se produit. Si une interface échoue sur les deux unités, les deux interfaces passent à l'état « Inconnu » et ne sont pas prises en compte dans la limite de basculement définie par la politique d'interface de basculement.

Une interface devient de nouveau opérationnelle si elle reçoit du trafic. Un ASA défaillant passe en mode veille si le seuil de défaillance de l'interface n'est plus atteint.

Si une interface a des adresses IPv4 et IPv6 configurées, le ASA utilise les adresses IPv4 pour effectuer la surveillance de l'intégrité. Si une interface n'a que des adresses IPv6 configurées, le ASA utilise la découverte des voisins IPv6 au lieu d'ARP pour effectuer les tests de surveillance de l'intégrité. Pour le test de ping de diffusion, le ASA utilise l'adresse de tous les nœuds IPv6 (FE02::1).

Remarque Si une unité défaillante ne récupère pas et que vous pensez qu'elle ne devrait pas tomber en panne, vous pouvez réinitialiser l'état en saisissant la commande « **failover reset** ». Si la condition de basculement persiste, l'unité échouera à nouveau.

Tests d'interface

LeASA Firewall Threat Defense utilise les tests d'interface suivants. La durée de chaque test est d'environ 1,5 seconde par défaut, ou de 1/16 du temps d'attente de l'interface de basculement (voir la commande **failover polltime interface** ou, pour le basculement actif/actif, la commande **interface-policy**).

1. Test de liaison (Active/En panne) : test de l'état de l'interface. Si le test de liaison active/désactivée indique que l'interface est en panne, l'ASA la considère comme ayant échoué et les tests s'arrêtent. Si l'état est Activé, l'ASA effectue le test d'activité réseau.
2. Test d'activité réseau : test d'activité réseau reçu. Au début du test, chaque unité efface son nombre de paquets reçus pour ses interfaces. Dès qu'une unité reçoit des paquets admissibles pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, l'ASA démarre le test ARP.
3. Test ARP : Un test des réponses ARP réussies. Chaque unité envoie une seule requête ARP pour l'adresse IP dans l'entrée la plus récente de son tableau ARP. Si l'unité reçoit une réponse ARP ou un autre trafic réseau pendant le test, l'interface est considérée comme opérationnelle. Si l'unité ne reçoit pas de réponse ARP, l'ASA envoie une seule requête ARP pour l'adresse IP dans l'entrée *suivante* du tableau ARP. Si l'unité reçoit une réponse ARP ou un autre trafic réseau pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, l'ASA démarre le test ping de diffusion.
4. Test de ping de diffusion : un test de réponses au ping réussies. Chaque unité envoie un message Ping de diffusion, puis compte tous les paquets reçus. Si l'unité reçoit des paquets pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, les tests recommencent avec le test ARP. Si les deux unités continuent de ne recevoir aucun trafic venant des tests ARP et de ping de diffusion, ces tests continueront à se dérouler à l'infini.

État d'interface

Les interfaces surveillées peuvent avoir l'état suivant :

- Inconnu : état initial. Cet état peut également signifier qu'il ne peut pas être déterminé.
- Normal : l'interface reçoit du trafic.
- En test : les messages Hello ne sont pas entendus sur l'interface pendant cinq cycles d'interrogation.
- Liaison en panne : l'interface ou le VLAN est administrativement inactif.
- Aucune liaison : le lien physique de l'interface est inactif.
- Échec : aucun trafic n'est reçu sur l'interface, mais le trafic est diffusé sur l'interface homologue.

détection

Les événements suivants déclenchent le basculement dans une paire à haute disponibilité Firepower :

- Plus de 50 % des instances Snort sur l'unité active sont en panne.
- L'espace disque de l'unité active est plein à plus de 90 %.
- La commande **no failover active** est exécutée sur l'unité active ou la commande **failover active** est exécutée sur l'unité de secours.

- L'unité active comporte plus d'interfaces défaillantes que l'unité en veille.
- La défaillance d'interface sur le périphérique actif dépasse le seuil configuré.

  Par défaut, la défaillance d'une seule interface entraîne le basculement. Vous pouvez modifier la valeur par défaut en configurant un seuil pour le nombre d'interfaces ou un pourcentage d'interfaces surveillées qui doivent échouer pour que le basculement se produise. Si le seuil est dépassé sur le périphérique actif, le basculement se produit. Si le seuil est dépassé sur le périphérique en veille, l'unité passe à l'état **Fail** (échec).

  Pour modifier les critères de basculement par défaut, saisissez la commande suivante en mode de configuration globale :

Tableau 13 :

Commande	Objectif
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	Modifie les critères de basculement par défaut. Lorsque vous spécifiez un nombre spécifique d'interfaces, l'argument *num* peut être compris entre 1 et 250. Lors de la spécification d'un pourcentage d'interfaces, l'argument *num* peut être compris entre 1 et 100.



Remarque Si vous basculez manuellement à l'aide de l'interface de ligne de commande ou de l'ASDM, ou si vous rechargez l'ASA, le basculement démarre immédiatement et n'est pas soumis aux minuteurs ci-dessous.

Tableau 14 : ASA

la condition de basculement	Minimum	Par défaut	Maximum
L'unité active n'est plus alimentée, le matériel tombe en panne, le logiciel est rechargé ou se bloque. Lorsque l'un de ces événements se produit, les interfaces surveillées ou le lien de basculement ne reçoivent aucun message Hello.	800 milliseconde	15 secondes	45 secondes
Lien de l'interface de la carte principale de l' unité active en panne.	500 millisecondes	5 secondes	15 secondes
Lien d'interface de module 4GE de l'unité active inactif.	2 secondes	5 secondes	15 secondes
L'interface de l'unité active est active, mais un problème de connexion entraîne des tests d'interface.	5 secondes	25 secondes	75 secondes

Synchronisation de la configuration

Le basculement comprend différents types de synchronisation de configuration.

Réplication de la configuration en cours d'exécution

La réplication de la configuration en cours d'exécution se produit lorsque l'un des périphériques de la paire de basculement ou les deux démarrent.

Dans le basculement actif/veille, les configurations sont toujours synchronisées de l'unité active avec l'unité en veille.

Dans le basculement actif/actif, quelle que soit l'unité de démarrage, elle obtient la configuration en cours d'exécution de l'unité qui démarre en premier, quelle que soit la désignation principale ou secondaire de l'unité de démarrage. Une fois que les deux unités sont opérationnelles, les commandes saisies dans l'espace d'exécution du système sont répliquées à partir de l'unité sur laquelle le groupe de basculement 1 est à l'état actif.

Lorsque l'unité de secours/seconde termine son démarrage initial, elle efface sa configuration en cours d'exécution (à l'exception des commandes **failover** nécessaires pour communiquer avec l'unité active) et l'unité active envoie sa configuration complète à l'unité de secours/seconde. Lorsque la réplication démarre, la console ASA sur l'unité active affiche le message « Début de la réplication de la configuration : envoi à l'unité jumelle » et lorsqu'elle est terminée, l'ASA affiche le message « Fin de la réplication de la configuration vers l'unité jumelle ». Selon la taille de la configuration, la réplication peut prendre de quelques secondes à plusieurs minutes.

Sur l'unité recevant la configuration, la configuration existe uniquement dans la mémoire en cours d'exécution. Vous devez enregistrer la configuration dans la mémoire flash en fonction de Enregistrer les modifications de configuration, à la page 40. Par exemple, dans le basculement actif/actif, saisissez la commande **write memory all** dans l'espace d'exécution du système sur l'unité qui a le groupe de basculement 1 à l'état actif. La commande est répliquée sur l'unité homologue, qui continue d'écrire sa configuration dans la mémoire flash.



Remarque Pendant la réplication, les commandes saisies sur l'unité qui envoie la configuration peuvent ne pas être répliquées correctement sur l'unité homologue, et les commandes saisies sur l'unité qui reçoit la configuration peuvent être remplacées par la configuration en cours de réception. Évitez de saisir des commandes sur l'une ou l'autre des unités de la paire de basculement pendant le processus de réplication de la configuration.

Réplication du fichier

La synchronisation de la configuration ne réplique pas les fichiers et composants de configuration suivants. Vous devez donc copier ces fichiers manuellement pour qu'ils correspondent :

- Images Secure Client (services client sécurisés)
- Images CSD
- Profils Secure Client (services client sécurisés)

  L'ASA utilise un fichier mis en mémoire cache pour le profil Secure Client (services client sécurisés) stocké dans cache:/stc/profiles, et non le fichier stocké dans le système de fichiers flash. Pour répliquer le profil Secure Client (services client sécurisés) sur l'unité en veille, effectuez l'une des opérations suivantes :

- Saisissez la commande **write standby** sur l'unité active.
- Réappliquez le profil sur l'unité active.
- Rechargez l'unité en veille.

- Autorités de certification (CA) locales
- Images ASA
- Images ASDM

Réplication de la commande

Après le démarrage, les commandes que vous saisissez sur l'unité active sont immédiatement répliquées sur l'unité de secours. Vous n'avez pas besoin d'enregistrer la configuration active dans la mémoire flash pour répliquer les commandes.

Dans le basculement actif/actif, des commandes saisies dans l'espace d'exécution du système sont répliquées à partir de l'unité sur laquelle le groupe de basculement 1 est à l'état actif.

Si lesde commandes ne sont pas saisies sur l'unité appropriée pour que la réplication des commandes puisse avoir lieu, les configurations ne seront plus synchronisées. Ces modifications pourraient être perdues lors de la prochaine synchronisation de la configuration initiale.

Les commandes suivantes sont répliquées sur l'ASA de secours :

- Toutes les commandes de configuration, à l'exception de **mode**, **firewall** et **failover lan unit**
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

Les commandes suivantes ne sont *pas* répliquées sur l'ASA de secours :

- Toutes les formes de la commande **copy**, à l'exception de **copy running-config startup-config**
- Toutes les formes de la commande **write**, à l'exception de **write memory**
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** et **pager**

Optimisation de la synchronisation et de la configuration

Lorsqu'un périphérique redémarre ou se reconnecte après une suspension ou une reprise du basculement, le périphérique qui rejoint le nœud efface la configuration en cours d'exécution. Le périphérique actif envoie alors l'intégralité de sa configuration au périphérique en phase de jonction afin de synchroniser complètement les configurations. Si le périphérique actif a une configuration importante, ce processus peut prendre plusieurs minutes.

La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration du périphérique en phase de jonction et du périphérique actif en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les périphériques actifs et en phase de jonction correspond, le périphérique en cours d'adhésion ignore la synchronisation complète de la configuration et rejoint la configuration du basculement. Cette fonctionnalité garantit un appairage plus rapide et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.

Directives et limites de l'optimisation de la configuration et de la synchronisation

- La fonctionnalité d'optimisation de la synchronisation de la configuration est activée par défaut.
- Le mode de contexte multiple de l'ASA prend en charge l'optimisation de la synchronisation de la configuration en partageant l'ordre des contextes lors de la synchronisation complète de la configuration, ce qui permet la comparaison de l'ordre des contextes lors de la jonction de nœuds suivante.
- Si vous configurez la phrase secrète et la clé IPsec de basculement, l'optimisation de la synchronisation de la configuration n'est pas effective, car la valeur de hachage calculée dans le périphérique actif et le périphérique en veille est différente.
- Si vous configurez le périphérique avec une ACL dynamique ou SNMPv3, l'optimisation de la synchronisation de la configuration n'est pas effective.
- Le périphérique actif synchronise la configuration complète avec le basculement des liaisons LAN comme comportement par défaut. Pendant les oscillations de basculement entre les périphériques actifs et en veille, l'optimisation de la synchronisation de la configuration n'est pas déclenchée et les périphériques effectuent une synchronisation complète de la configuration.
- L'optimisation de la synchronisation de la configuration est déclenchée lorsque la configuration du basculement récupère d'une interruption ou d'une perte de communication réseau entre les périphériques actifs et en veille.

Surveillance de l'optimisation de la configuration et de la synchronisation

Lorsque la fonctionnalité d'optimisation de la synchronisation de la configuration est activée, des messages de journal système sont générés pour indiquer si les valeurs de hachage calculées sur l'unité active et en phase de jonction correspondent, ne correspondent pas ou si le délai de l'opération expire. Le message syslog affiche également le temps écoulé, depuis l'envoi de la demande de hachage jusqu'au moment d'obtenir et de comparer la réponse de hachage.

Utilisez les commandes suivantes pour superviser l'optimisation de la synchronisation de la configuration.

- **show failover config-sync checksum**

  Affiche des informations sur l'état du périphérique et la somme de contrôle.

- **show failover config-sync configuration**

  Affiche des informations sur la configuration du périphérique et la somme de contrôle.

- **show failover config-sync status**

  Affiche l'état de la fonctionnalité d'optimisation de la synchronisation de la configuration.

À propos du basculement actif/de secours

Le basculement actif/en veille vous permet d'utiliser un ASA de secours pour reprendre les fonctionnalités d'une unité en panne. Lorsque l'unité active tombe en panne, l'unité en veille devient l'unité active. Cependant, vous devez définir l'unité de secours comme unité principale avant de remplacer l'unité défectueuse, afin de conserver la configuration de l'unité secondaire.



Remarque Pour le mode de contexte multiple, l'ASA peut basculer l'unité entière (y compris tous les contextes), mais ne peut pas basculer des contextes individuels séparément.

Rôles principal/secondaire et état actif/de secours

Les principales différences entre les deux unités d'une paire de basculement dépendent de l'unité active et de l'unité en veille, à savoir les adresses IP à utiliser et l'unité transmettant activement le trafic.

Cependant, il existe quelques différences entre les unités en fonction de l'unité principale (comme spécifié dans la configuration) et de l'unité secondaire :

- L'unité principale devient toujours l'unité active si les deux unités démarrent en même temps (et ont le même état de fonctionnement opérationnel).
- Les adresses MAC de l'unité principale sont toujours associées aux adresses IP actives. L'exception à cette règle se produit lorsque l'unité secondaire devient active et ne peut pas obtenir les adresses MAC de l'unité principale sur la liaison de basculement. Dans ce cas, les adresses MAC des unités secondaires sont utilisées.

Détermination de l'unité active au démarrage

L'unité active est déterminée par les éléments suivants :

- Si une unité démarre et détecte un homologue qui fonctionne déjà comme actif, elle devient l'unité de secours.
- Si une unité démarre et ne détecte pas d'homologue, elle devient l'unité active.
- Si les deux unités démarrent simultanément, l'unité principale devient l'unité active et l'unité secondaire devient l'unité de secours.

Événements de basculement

Dans le cas d'un basculement actif/de secours, le basculement se produit de manière unitaire. Même sur les systèmes exécutés dans le mode à contextes multiples, vous ne pouvez pas basculer des contextes ou des groupes de contextes.

Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque défaillance, le tableau indique la politique de basculement (basculement ou absence de basculement), l'action prise par l'unité

active, l'action entreprise par l'unité de secours, et toute remarque spéciale sur la condition et les actions de basculement.

Tableau 15 : Événements de basculement

Défaillance	Politique	Action de l'unité active	Action de l'unité de secours	Notes
Défaillance de l'unité active (alimentation ou matérielle)	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante	Aucun message Hello n'est reçu sur l'interface surveillée ou sur la liaison de basculement.
L'unité précédemment active récupère	Aucun basculement	Devient l'unité de secours	Aucune action	Aucun.
Défaillance de l'unité de secours (alimentation ou matériel)	Aucun basculement	Marquer l'unité de secours come défaillante	S.O.	Lorsque l'unité de secours est marquée comme défaillante, l'unité active ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.
Échec du la liaison de basculement pendant l'opération	Aucun basculement	Marquer la liaison de basculement comme défaillante	Marquer la liaison de basculement comme défaillante	Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer vers l'unité de secours lorsque la liaison de basculement est inactive.
Échec de la liaison de basculement au démarrage	Aucun basculement	Devenir active Marquer la liaison de basculement comme défaillante	Devenir active Marquer la liaison de basculement comme défaillante	Si la liaison de basculement est interrompue au démarrage, les deux unités deviennent actives.
Échec du lien avec l'état	Aucun basculement	Aucune action	Aucune action	Les informations d'état deviennent obsolètes et les sessions sont interrompues en cas de basculement.
Défaillance de l'interface sur l'unité active supérieure au seuil	Basculement	Marquer l'unité active comme défaillante	Devenir active	Aucun.
Défaillance de l'interface sur l'unité de secours supérieure au seuil	Aucun basculement	Aucune action	Marquer l'unité de secours come défaillante	Lorsque l'unité de secours est marquée comme en panne, l'unité active ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.

À propos du basculement actif/actif

Cette section décrit le basculement actif/actif.

Présentation du basculement actif/actif

Dans une configuration de basculement actif/actif, les deux ASA peuvent transmettre le trafic réseau. Le basculement actif/actif n'est disponible que pour les ASA en mode de contexte multiple. Dans le basculement actif/actif, vous divisez les contextes de sécurité sur l'ASA en un maximum de 2 groupes de basculement.

Un groupe de basculement est simplement un groupe logique d'un ou plusieurs contextes de sécurité. Vous pouvez attribuer un groupe de basculement actif sur l'ASA principal et un groupe de basculement 2 actif sur l'ASA secondaire. Lorsqu'un basculement se produit, il se produit au niveau du groupe de basculement. Par exemple, selon le modèle de défaillance d'interface, il est possible que le groupe de basculement 1 bascule vers l'ASA secondaire et que le groupe de basculement 2 bascule vers l'ASA principal. Cet événement peut se produire si les interfaces du groupe de basculement 1 sont inactives sur l'ASA principal, mais actives sur l'ASA secondaire, tandis que les interfaces du groupe de basculement 2 sont inactives sur l'ASA secondaire, mais actives sur l'ASA principal.

Le contexte d'administration est toujours membre du groupe de basculement 1. Tous les contextes de sécurité non attribués sont également membres du groupe de basculement 1 par défaut. Si vous souhaitez bénéficier d'un basculement actif/actif, mais que vous n'êtes pas intéressé par les contextes multiples, la configuration la plus simple serait d'ajouter un contexte supplémentaire et de l'affecter au groupe de basculement 2.

Remarque Lors de la configuration du basculement actif/actif, assurez-vous que le trafic combiné des deux unités entre dans la capacité de chacune d'elles.

Remarque Vous pouvez attribuer les deux groupes de basculement à un seul ASA si vous le souhaitez, mais vous ne profiterez pas de deux ASA actifs.

Rôles principal/secondaire et état actif/de secours pour un groupe de basculement

Comme pour le basculement actif/de secours, une unité d'une paire de basculement actif/actif est désignée comme l'unité principale et l'autre unité, comme l'unité secondaire. Contrairement au basculement actif/de secours, cette désignation n'indique pas quelle unité devient active lorsque les deux unités démarrent simultanément. Au lieu de cela, la désignation principale/secondaire fait deux choses :

- L'unité principale fournit la configuration d'exécution à la paire lorsqu'elles démarrent simultanément.
- Chaque groupe de basculement de la configuration est configuré avec une préférence d'unité principale ou secondaire. Lorsqu'elle est utilisée avec la préemption, cette préférence garantit que le groupe de basculement s'exécute sur la bonne unité après son démarrage. Sans préemption, les deux groupes s'exécutent sur la première unité de démarrage.

Détermination de l'unité active pour les groupes de basculement au démarrage

L'unité sur laquelle un groupe de basculement devient actif est déterminée comme suit :

- Lorsqu'une unité démarre alors que l'unité homologue n'est pas disponible, les deux groupes de basculement deviennent actifs sur l'unité.

- Lorsqu'une unité démarre alors que l'unité homologue est active (avec les deux groupes de basculement à l'état actif), les groupes de basculement restent à l'état actif sur l'unité active, quelle que soit la préférence principale ou secondaire du groupe de basculement jusqu'à ce que l'un des scénarios suivants se produise :
  - Un basculement se produit.
  - Un basculement est forcé manuellement.
  - Une préemption pour le groupe de basculement est configurée, ce qui fait que le groupe de basculement devient automatiquement actif sur l'unité préférée lorsque l'unité devient disponible.

Événements de basculement

Dans une configuration de basculement actif/actif, le basculement se produit sur la base d'un groupe de basculement, et non sur une base de système. Par exemple, si vous désignez les deux groupes de basculement comme actifs sur l'unité principale et que le groupe de basculement 1 échoue, le groupe de basculement 2 reste actif sur l'unité principale pendant que le groupe de basculement 1 devient actif sur l'unité secondaire.

Comme un groupe de basculement peut contenir plusieurs contextes et que chaque contexte peut contenir plusieurs interfaces, il est possible que toutes les interfaces d'un contexte unique tombent en panne sans entraîner la défaillance du groupe de basculement associé.

Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque événement de défaillance, la politique (que le basculement se produise ou non), les actions pour le groupe de basculement actif et les actions pour le groupe de basculement en veille sont données.

Tableau 16 : Événements de basculement

Défaillance	Politique	Action pour le groupe actif	Action pour le groupe en veille	Notes
Une unité subit une défaillance d'alimentation ou de logiciel	Basculement	Devient l'unité de secours Marquer comme défaillante	Devenir active Marquer l'unité active comme défaillante	Lorsqu'une unité d'une paire de basculement tombe en panne, tous les groupes de basculement actifs sur cette unité sont marqués comme défaillants et deviennent actifs sur l'unité homologue.
Défaillance de l'interface sur le groupe de basculement actif supérieure au seuil	Basculement	Marquer le groupe actif comme défaillant	Devenir active	Aucun.
Défaillance de l'interface sur le groupe de basculement en veille supérieure au seuil	Aucun basculement	Aucune action	Marquer le groupe en veille comme défaillant	Lorsque le groupe de basculement en veille est marqué comme défaillant, le groupe de basculement actif ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.
Le groupe de basculement anciennement actif récupère	Aucun basculement	Aucune action	Aucune action	À moins que la préemption de groupe de basculement ne soit configurée, les groupes de basculement restent actifs sur leur unité actuelle.

Défaillance	Politique	Action pour le groupe actif	Action pour le groupe en veille	Notes
Échec de la liaison de basculement au démarrage	Aucun basculement	Devenir active	Devenir active	Si la liaison de basculement est interrompue au démarrage, les deux groupes de basculement sur les deux unités deviennent actifs.
Échec du lien avec l'état	Aucun basculement	Aucune action	Aucune action	Les informations d'état deviennent obsolètes et les sessions sont interrompues en cas de basculement.
Échec du la liaison de basculement pendant l'opération	Aucun basculement	S.O.	S.O.	Chaque unité marque la liaison de basculement comme défaillante. Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer vers l'unité de secours lorsque la liaison de basculement est inactive.

Licences pour le basculement

Pour la plupart des modèles, les unités de basculement ne nécessitent pas la même licence sur chaque unité. Si vous avez des licences sur les deux unités, elles se combinent en une seule licence de grappe de basculement d'exécution. Il y a certaines exceptions à cette règle. Consultez le tableau suivant pour connaître les exigences précises en matière de licence pour le basculement.

Modèle	Exigence de licence
ASA virtuel	Consultez Licences de basculement pour l'ASAv, à la page 101.
Firepower 1010	Licence Security Plus sur les deux unités. Consultez Licences de basculement pour Firepower 1010, à la page 102.
Firepower 1100	Consultez Licences de basculement pour Firepower 1100, à la page 102.
Firepower de la série 2100	Consultez Licences de basculement pour Firepower 2100, à la page 104.
Cisco Secure Firewall 3100	Consultez Licences de basculement pour Cisco Secure Firewall 3100, à la page 105.
Firepower 4100/9300	Consultez Licences de basculement pour l'Firepower 4100/9300, à la page 107.
ISA 3000	Licence Security Plus sur les deux unités. **Remarque** Chaque unité doit avoir la même licence de chiffrement.

Remarque Une clé permanente valide est requise; dans de rares cas sur l'ISA 3000, votre clé d'authentification PAK peut être supprimée. Si votre clé est constituée uniquement de 0, vous devez réinstaller une clé d'authentification valide avant que le basculement puisse être activé.

Lignes directrices pour Failover (basculement)

Mode contextuel

- Le mode Actif/Actif est pris en charge uniquement en mode de contexte multiple.
- Pour le mode de contexte multiple, effectuez toutes les étapes dans l'espace d'exécution du système, sauf indication contraire.

Prise en charge des modèles

- Firepower 1010 :
  - Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de Failover (basculement). Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. Failover (basculement) est conçu pour empêcher le trafic de passer par l'unité en veille, mais cette fonctionnalité ne s'étend pas aux ports de commutation. Dans une configuration réseau Failover (basculement) normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d'utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser Failover (basculement) avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
  - Vous ne pouvez utiliser qu'une interface de pare-feu comme liaison de basculement.
- Firepower 9300 : nous vous recommandons d'utiliser le basculement entre les châssis pour une redondance optimale.
- Les ASA virtuel sur les réseaux infonuagiques publics tels que Microsoft Azure et Amazon Web Services ne sont pas pris en charge par Failover (basculement) standard, car une connectivité de couche 2 est requise. Au lieu de cela, consultez Basculement pour la haute disponibilité dans le nuage public, à la page 331.

Basculement ASA virtuel pour la haute disponibilité

Lors de la création d'une paire de basculement à l'aide de l'ASA virtuel, il est nécessaire d'ajouter les interfaces de données à chaque ASA virtuel dans le même ordre. Si exactement les mêmes interfaces sont ajoutées à chaque ASA virtuel, mais dans un ordre différent, des erreurs peuvent s'afficher à la console ASA virtuel. La fonctionnalité de basculement peut également être affectée

Directives supplémentaires

- Lorsque l'unité active bascule sur l'unité en veille, le port du commutateur connecté exécutant le protocole Spanning Tree (STP) peut passer dans un état bloquant pendant 30 à 50 secondes lorsqu'il détecte le changement de topologie. Pour éviter la perte de trafic lorsque le port est dans un état bloquant, vous pouvez activer la fonctionnalité STP PortFast sur le commutateur :

  interface *interface_id* **spanning-tree portfast**

  Cette solution de contournement s'applique aux commutateurs connectés aux interfaces du mode routé et de groupe de ponts. La fonctionnalité PortFast fait immédiatement passer le port en mode de transfert STP lors de l'établissement de la liaison. Le port participe toujours à STP. Ainsi, si le port doit faire partie de la boucle, le port finit par passer en mode de blocage STP.

- La configuration de la sécurité des ports sur les commutateurs connectés à la paire de basculement ASA peut entraîner des problèmes de communication lors d'un basculement. Ce problème se produit lorsqu'une adresse MAC sécurisée configurée ou apprise sur un port sécurisé est déplacée vers un autre port sécurisé. Une violation est signalée par la fonctionnalité de sécurité du port du commutateur.

- Vous pouvez surveiller jusqu'à 1 025 interfaces sur une unité, dans tous les contextes.

- Pour un tunnel Failover (basculement) actif/en veille et un tunnel VPN IPsec, vous ne pouvez pas surveiller les unités active et en veille à l'aide de SNMP sur le tunnel VPN. L'unité de secours n'a pas de tunnel VPN actif et abandonnera le trafic destiné au système NMS. Vous pouvez plutôt utiliser SNMPv3 avec chiffrement pour que le tunnel IPsec ne soit pas requis.

- Pour le basculement actif/actif, deux interfaces dans le même contexte ne doivent pas être configurées dans le même groupe ASR.

- Pour le basculement actif/actif, vous pouvez définir un maximum de deux groupes de basculement.

- Pour le basculement actif/actif, lors de la suppression de groupes de basculement, vous devez supprimer le groupe de basculement 1 en dernier. Le groupe de basculement1 contient toujours le contexte d'administration. Tout contexte non affecté à un groupe de basculement passe par défaut au groupe de basculement 1. Vous ne pouvez pas supprimer un groupe de basculement auquel des contextes sont affectés explicitement.

- Immédiatement après le basculement, l'adresse source des messages du journal système sera l'adresse de l'interface de basculement pendant quelques secondes.

- Pour une meilleure convergence (pendant un basculement), vous devez fermer les interfaces sur une paire à haute disponibilité qui ne sont associées à aucune configuration ou instance.

- Si vous configurez le chiffrement de basculement en mode d'évaluation, les systèmes utilisent DES pour le chiffrement. Si vous enregistrez ensuite les périphériques à l'aide d'un compte compatible avec l'exportation, ils utiliseront AES après un redémarrage. Ainsi, si un système redémarre pour une raison quelconque, y compris après l'installation d'une mise à niveau, les homologues ne pourront pas communiquer et les deux unités deviendront l'unité active. Nous vous recommandons de ne pas configurer le chiffrement avant d'avoir enregistré les périphériques. Si vous configurez cela en mode d'évaluation, nous vous recommandons de supprimer le chiffrement avant d'enregistrer les périphériques.

- Lorsque vous utilisez SNMPv3 avec basculement, si vous remplacez une unité de basculement, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez rajouter les utilisateurs SNMPv3 à l'unité active pour forcer les utilisateurs à se reproduire sur la nouvelle unité; ou vous pouvez ajouter les utilisateurs directement sur la nouvelle unité. Reconfigurez chaque utilisateur en saisissant la commande **snmp-server user** *username group-name* **v3** sur l'unité active ou directement sur l'unité de secours avec les options *priv-password* et *auth-password* dans leur format non chiffré.

- Le périphérique ne partage pas les données du moteur client SNMP avec son homologue.
- Si vous avez un très grand nombre de règles de contrôle d'accès et de NAT, la taille de la configuration peut empêcher une duplication efficace de la configuration, ce qui se traduit par le fait que l'unité de secours met trop de temps à atteindre l'état de veille. Cela peut également avoir une incidence sur votre capacité à vous connecter à l'unité de secours pendant la duplication via la console ou la session SSH. Pour améliorer les performances de duplication de la configuration, activez la validation transactionnelle pour les règles d'accès et la NAT à l'aide des commandes **asp rule-engine transactional-commit access-group** et **asp rule-engine transactional-commit nat**.
- Une unité d'une paire Failover (basculement) qui passe en rôle de secours synchronise son horloge avec celle de l'unité active.

  Exemple :

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby              Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config               Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- Les unités de Failover (basculement) ne synchronisent pas l'horloge de manière dynamique. Voici quelques exemples d'événements où la synchronisation a lieu :
  - Une nouvelle paire Failover (basculement) est créée.
  - La paire Failover (basculement) est défectueuse et recréée.
  - La communication sur la liaison de basculement a été interrompue et rétablie.
  - L'état de basculement a été modifié manuellement au niveau de l'interface de ligne de commande (CLI) .
- L'activation de Failover (basculement) force la suppression de toutes les routes et leur rajout après le passage de la progression de Failover (basculement) à l'état actif. Vous pourriez subir des pertes de connexion pendant cette phase.
- Si vous activez le basculement sur un périphérique autonome, les interfaces de données tombent en panne lors de la négociation du basculement, interrompant le trafic.
- Dans la configuration Failover (basculement), les connexions de courte durée, généralement qui utilisent le port 53, sont fermées rapidement et ne sont jamais transférées ou synchronisées de la position active à la zone en veille, il peut donc y avoir une différence dans le nombre de connexions sur les deux périphériques Failover (basculement). C'est un comportement attendu pour les connexions de courte durée. Vous pouvez essayer de comparer les connexions qui sont de longue durée (par exemple, plus de 30 à 60 secondes).
- Dans la configuration Failover (basculement), les connexions amorces (demandes de connexion qui n'ont pas encore terminé le processus d'établissement de liaison à trois étapes) sont fermées rapidement et ne sont pas synchronisées entre les périphériques actifs et en veille. Cette conception garantit l'efficacité et

la sécurité du système à haute disponibilité. Pour cette raison, il pourrait y avoir une différence dans le nombre de connexions sur les deux périphériques Failover (basculement), ce qui est attendu.

- Si la liaison LAN de basculement n'est pas connectée dos à dos, mais plutôt connectée par un ou plusieurs commutateurs, une défaillance dans le chemin intermédiaire peut faire que l'unité active perde la connectivité avec l'unité de secours, ce qui entraîne des états actif/veille incohérents. Bien que cela n'ait pas d'incidence sur la fonctionnalité Failover (basculement), il est conseillé de vérifier et de récupérer le chemin de liaison de basculement entre les unités actives et de secours.

  Lorsque la liaison LAN de basculement est inactive, il n'est pas conseillé de déployer une configuration, car elle pourrait ne pas être répliquée sur l'unité homologue.

- Dans OSPF dans l'ASA, si un commutateur à proximité tombe en panne et si l'interface ASA est connectée au même commutateur, les interfaces du pare-feu tombent également en panne avec la défaillance du commutateur. Il s'agit d'un comportement attendu. Cela déclenchera un basculement de haute disponibilité, comme prévu.

- Si l'ASA en veille est connecté à un autre commutateur, par exemple, lorsque l'interface sera activée, les tables de routage seront différentes de celle de l'ASA actif. Cela entraînera une panne de courte durée (environ 15 à 17 secondes) jusqu'à ce que les routes et la contiguïté soient mises à jour.

- En mode transparent, si vous avez des problèmes avec l'unité active qui perd l'adresse MAC du routeur de secours (HSRP), créez un mappage statique pour l'adresse MAC.

Paramètres par défaut pour le basculement

Par défaut, la politique de basculement comprend les éléments suivants :

- Aucune réplication HTTP dans le basculement dynamique.
- La défaillance d'une seule interface entraîne le basculement.
- Le délai d'interrogation de l'interface est de 5 secondes.
- Le délai de rétention de l'interface est de 25 secondes.
- Le délai d'interrogation de l'unité est de 1 seconde.
- Le délai de rétention de l'unité est de 15 secondes.
- Les adresses MAC virtuelles sont désactivées en mode de contexte multiple.
- Supervision de toutes les interfaces physiques.

Configurer le basculement actif/de secours

Pour configurer le basculement actif/veille, configurez les paramètres de basculement de base sur les unités principale et secondaire. Toutes les autres configurations se produisent uniquement sur l'unité principale et sont ensuite synchronisées avec l'unité secondaire.

Configurer l'unité principale pour le basculement actif/de secours

Suivez les étapes de cette section pour configurer l'unité principale dans une configuration de basculement actif/veille. Ces étapes fournissent la configuration minimum nécessaire pour activer le basculement sur l'unité principale.

Avant de commencer

- Nous vous conseillons de configurer les adresses IP en veille pour toutes les interfaces, à l'exception des liaisons de basculement et d'état. Si vous utilisez un filtre d'adresse locale de 31 bits pour les connexions point à point, ne configurez pas d'adresse IP en veille. Vous ne pourrez pas activer le basculement si des interfaces sont configurées pour DHCP.
- Ne configurez pas d'argument **nameif** pour les liaisons de basculement et d'état.
- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Désignez cette unité comme unité principale :

failover lan unit primary

Étape 2 Spécifiez l'interface à utiliser comme liaison de basculement :

failover lan interface *if_name interface_id*

Exemple :

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

Cette interface ne peut pas être utilisée à d'autres fins (sauf, éventuellement, pour la liaison d'état).

L'argument *if_name* attribue un nom à l'interface.

L'argument *interface_id* peut être une interface physique de données, une sous-interface ou un ID d'interface EtherChannel. Sur Firepower 1010, l'interface est un ID d'interface de pare-feu; vous ne pouvez pas spécifier d'ID de port de commutation ni d'ID de VLAN. Pour le Firepower 4100/9300, vous pouvez utiliser n'importe quelle interface de type de données.

Étape 3 Attribuez les adresses IP actives et en veille à la liaison de basculement :

failover interface ip *failover_if_name* {*ip_address mask* | *ipv6_address* / *prefix*} **standby** *ip_address*

Exemple :

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Ou :

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
```

```
2001:a0a:b00::a0a:b71
```

Cette adresse doit se trouver sur un sous-réseau inutilisé. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.

L'adresse IP en veille doit se trouver dans le même sous-réseau que l'adresse IP active.

Étape 4 Activez la liaison de basculement :

interface *failover_interface_id*

no shutdown

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

Étape 5 (Facultatif) Si vous souhaitez utiliser une interface distincte pour la liaison d'état, spécifiez l'interface.

failover link *if_name interface_id*

Exemple :

```
ciscoasa(config)# failover link folink gigabitethernet0/4
```

Si vous ne spécifiez pas d'interface distincte, la liaison de basculement est utilisée pour la liaison d'état.

L'argument *if_name* attribue un nom à l'interface.

L'argument *interface_id* peut être une interface physique, une sous-interface ou un ID d'interface EtherChannel. Sur Firepower 1010, l'interface est un ID d'interface de pare-feu; vous ne pouvez pas spécifier d'ID de port de commutation ni d'ID de VLAN.

Étape 6 Si vous avez spécifié une liaison d'état distincte, attribuez les adresses IP actives et en veille à cette liaison d'état :

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

Exemple :

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

Ou :

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

Cette adresse doit se trouver sur un sous-réseau inutilisé, différent de la liaison de basculement. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.

L'adresse IP en veille doit se trouver dans le même sous-réseau que l'adresse IP active.

Ignorez cette étape si vous partagez la liaison d'état.

Étape 7 Si vous avez spécifié une liaison d'état distincte, activez cette dernière.

interface *state_interface_id*

no shutdown

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

Ignorez cette étape si vous partagez la liaison d'état.

Étape 8 (Facultatif) Effectuez l'une des opérations suivantes pour chiffrer les communications sur les liaisons de basculement et d'état :

- (Privilégié) Établissez des tunnels IPsec LAN à LAN sur les liaisons de basculement et d'état entre les unités pour chiffrer toutes les communications de basculement :

  failover ipsec pre-shared-key [**0** | **8**] *key*

  Exemple :

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  La *clé* peut comporter jusqu'à 128 caractères. Identifiez la même clé sur les deux unités. La clé est utilisée par IKEv2 pour établir les tunnels.

  Si vous utilisez une phrase secrète principale (voir Configurer la phrase secrète principale, à la page 840), la clé est chiffrée dans la configuration. Si vous copiez à partir de la configuration (par exemple, à partir de la sortie **more system:running-config**), spécifiez que la clé est chiffrée à l'aide du mot clé **8**. **0** est utilisé par défaut, spécifiant un mot de passe non chiffré.

  La clé partagée **failover ipsec pre-shared-key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée.

  Si vous ne configurez pas le chiffrement des liaisons de basculement et d'état, la communication de basculement, y compris tous les mots de passe ou clés de la configuration qui sont envoyés lors de la réplication des commandes, sera en texte clair.

  Vous ne pouvez pas utiliser à la fois le chiffrement IPsec et le chiffrement **failover key** existant. Si vous configurez les deux méthodes, IPsec est utilisé. Cependant, si vous utilisez la phrase secrète principale, vous devez d'abord supprimer la clé de basculement à l'aide de la commande **no failover key** avant de configurer le chiffrement IPsec.

  Les tunnels de basculement LAN à LAN ne sont pas pris en compte dans la licence IPsec (autre VPN).

- (Facultatif) Chiffrez la communication de basculement sur les liaisons de basculement et d'état :

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  Exemple :

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

Utilisez un *shared_secret* de 1 à 63 caractères ou une **hex** *key* de 32 caractères. Pour le *shared_secret*, vous pouvez utiliser n'importe quelle combinaison de chiffres, de lettres ou de ponctuation. Le secret partagé ou la clé hexadécimale est utilisé pour générer la clé de chiffrement. Identifiez la même clé sur les deux unités.

Si vous utilisez une phrase secrète principale (voir Configurer la phrase secrète principale, à la page 840), le secret partagé ou la clé hexadécimale est chiffré dans la configuration. Si vous copiez à partir de la configuration (par exemple, à partir de la sortie **more system:running-config**), spécifiez que le secret partagé ou la clé hexadécimale est chiffré à l'aide du mot clé **8**. **0** est utilisé par défaut, spécifiant un mot de passe non chiffré.

Le secret partagé **failover key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée.

Si vous ne configurez pas le chiffrement des liaisons de basculement et d'état, la communication de basculement, y compris tous les mots de passe ou clés de la configuration qui sont envoyés lors de la réplication des commandes, sera en texte clair.

Étape 9 Activez le basculement :

failover

Étape 10 Enregistrez la configuration système dans la mémoire flash :

write memory

Exemples

L'exemple suivant configure les paramètres de basculement pour l'unité principale :

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

Configurer l'unité secondaire pour le basculement actif/de secours

La seule configuration requise sur l'unité secondaire concerne la liaison de basculement. L'unité secondaire exige que ces commandes communiquent initialement avec l'unité principale. Une fois que l'unité principale a envoyé sa configuration à l'unité secondaire, la seule différence permanente entre les deux configurations est la commande **basculement LAN unité**, qui identifie chaque unité comme principale ou secondaire.

Avant de commencer

- Vous ne pourrez pas activer le basculement si des interfaces sont configurées pour DHCP.
- Ne configurez pas d'argument **nameif** pour les liaisons de basculement et d'état.

- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Saisissez à nouveau les mêmes commandes que sur l'unité principale, *à l'exception* de la commande **basculement LAN unité principale**. Vous pouvez éventuellement la remplacer par la commande **basculement LAN unité secondaire**, mais ce n'est pas nécessaire, car **le paramètre secondaire** est le paramètre par défaut. Consultez Configurer l'unité principale pour le basculement actif/de secours, à la page 300.

Par exemple :

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-ifc)# no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

Étape 2 Après la synchronisation de la configuration de basculement, enregistrez la configuration dans la mémoire flash :

```
ciscoasa(config)# write memory
```

Configurer le basculement actif/actif

Cette section explique comment configurer le basculement actif/actif.

Configurer l'unité principale pour le basculement actif/actif

Suivez les étapes de cette section pour configurer l'unité principale dans une configuration de basculement actif/actif. Ces étapes fournissent la configuration minimum nécessaire pour activer le basculement sur l'unité principale.

Avant de commencer

- Activez ou désactivez le mode de contexte multiple conformément à Activer ou désactiver le mode de contexte multiple, à la page 240.
- Nous vous conseillons de configurer les adresses IP en veille pour toutes les interfaces, à l'exception des liaisons de basculement et d'état conformément à Interfaces en mode routage et en mode transparent, à la page 763. Si vous utilisez un filtre d'adresse locale de 31 bits pour les connexions point à point, ne configurez pas d'adresse IP en veille. Vous ne pourrez pas activer le basculement si des interfaces sont configurées pour DHCP.

- Ne configurez pas d'argument **nameif** pour les liaisons de basculement et d'état.
- Effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Désignez cette unité comme unité principale :

failover lan unit primary

Étape 2 Spécifiez l'interface à utiliser comme liaison de basculement :

failover lan interface *if_name interface_id*

Exemple :

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

Cette interface ne peut pas être utilisée à d'autres fins (sauf, éventuellement, pour la liaison d'état).

L'argument *if_name* attribue un nom à l'interface.

L'argument *interface_id* peut être une interface physique, une sous-interface ou un ID d'interface EtherChannel. Pour le Firepower 4100/9300, vous pouvez utiliser n'importe quelle interface de type de données.

Étape 3 Attribuez les adresses IP actives et en veille à la liaison de basculement :

standby failover interface ip *if_name* {*ip_address mask* | *ipv6_address*/*prefix* } **standby** *ip_address*

Exemple :

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Ou :

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

Cette adresse doit se trouver sur un sous-réseau inutilisé. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.

L'adresse IP en veille doit se trouver dans le même sous-réseau que l'adresse IP active.

Étape 4 Activez la liaison de basculement :

interface *failover_interface_id*

no shutdown

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/3
```

```
ciscoasa(config-if)# no shutdown
```

Étape 5 (Facultatif) Si vous souhaitez utiliser une interface distincte pour la liaison d'état, spécifiez l'interface.

failover link *if_name interface_id*

Exemple :

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

Nous vous conseillons d'utiliser une liaison d'état distincte de la liaison de basculement. Si vous ne spécifiez pas d'interface distincte, la liaison de basculement est utilisée pour la liaison d'état.

L'argument *if_name* attribue un nom à l'interface.

L'argument *interface_id* peut être une interface physique, une sous-interface ou un ID d'interface EtherChannel.

Étape 6 Si vous avez spécifié une liaison d'état distincte, attribuez les adresses IP actives et en veille à cette liaison d'état :

Cette adresse doit se trouver sur un sous-réseau inutilisé, différent de la liaison de basculement. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.

L'adresse IP en veille doit se trouver dans le même sous-réseau que l'adresse IP active.

Ignorez cette étape si vous partagez la liaison d'état.

failover interface ip state *if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

Exemple :

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

Ou :

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

Étape 7 Si vous avez spécifié une liaison d'état distincte, activez cette dernière :

interface *state_interface_id*

no shutdown

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

Ignorez cette étape si vous partagez la liaison d'état.

Étape 8 (Facultatif) Effectuez l'une des opérations suivantes pour chiffrer les communications sur les liaisons de basculement et d'état :

- (Privilégié) Établissez des tunnels IPsec LAN à LAN sur les liaisons de basculement et d'état entre les unités pour chiffrer toutes les communications de basculement :

  failover ipsec pre-shared-key [**0** | **8**] *key*

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  La *clé* peut comporter jusqu'à 128 caractères. Identifiez la même clé sur les deux unités. La clé est utilisée par IKEv2 pour établir les tunnels.

  Si vous utilisez une phrase secrète principale (voir Configurer la phrase secrète principale, à la page 840), la clé est chiffrée dans la configuration. Si vous copiez à partir de la configuration (par exemple, à partir de la sortie **more system:running-config**), spécifiez que la clé est chiffrée à l'aide du mot clé **8**. **0** est utilisé par défaut, spécifiant un mot de passe non chiffré.

  La clé partagée **failover ipsec pre-shared-key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée.

  Si vous ne configurez pas le chiffrement des liaisons de basculement et d'état, la communication de basculement, y compris tous les mots de passe ou clés de la configuration qui sont envoyés lors de la réplication des commandes, sera en texte clair.

  Vous ne pouvez pas utiliser à la fois le chiffrement IPsec et le chiffrement **failover key** existant. Si vous configurez les deux méthodes, IPsec est utilisé. Cependant, si vous utilisez la phrase secrète principale, vous devez d'abord supprimer la clé de basculement à l'aide de la commande **no failover key** avant de configurer le chiffrement IPsec.

  Les tunnels de basculement LAN à LAN ne sont pas pris en compte dans la licence IPsec (autre VPN).

- (Facultatif) Chiffrez la communication de basculement sur les liaisons de basculement et d'état :

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  Utilisez un *shared_secret*, de 1 à 63 caractères, ou une **hex** *key* de 32 caractères.

  Pour le *shared_secret*, vous pouvez utiliser n'importe quelle combinaison de chiffres, de lettres ou de ponctuation. Le secret partagé ou la clé hexadécimale est utilisé pour générer la clé de chiffrement. Identifiez la même clé sur les deux unités.

  Si vous utilisez une phrase secrète principale (voir Configurer la phrase secrète principale, à la page 840), le secret partagé ou la clé hexadécimale est chiffré dans la configuration. Si vous copiez à partir de la configuration (par exemple, à partir de la sortie **more system:running-config**), spécifiez que le secret partagé ou la clé hexadécimale est chiffré à l'aide du mot clé **8**. **0** est utilisé par défaut, spécifiant un mot de passe non chiffré.

  Le secret partagé **failover key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée.

  Si vous ne configurez pas le chiffrement des liaisons de basculement et d'état, la communication de basculement, y compris tous les mots de passe ou clés de la configuration qui sont envoyés lors de la réplication des commandes, sera en texte clair.

Étape 9 Créez un groupe de basculement 1 :

failover group 1

primary

preempt [*delay*]

Exemple :

```
ciscoasa(config-fover-group)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 1200
```

En règle générale, vous affectez le groupe 1 à l'unité principale et le groupe 2 à l'unité secondaire. Les deux groupes de basculement deviennent actifs sur l'unité qui démarre en premier (même s'il semble qu'ils démarrent simultanément, une unité devient active en premier), malgré le paramètre principal ou secondaire du groupe. La commande **preempt** active le groupe de basculement sur l'unité désignée automatiquement lorsque cette unité est disponible.

Vous pouvez saisir une valeur *delay* facultative, qui spécifie le nombre de secondes pendant lesquelles le groupe de basculement reste actif sur l'unité actuelle avant de devenir automatiquement actif sur l'unité désignée. Cette valeur peut être comprise entre 1 et 1 200.

Si le basculement dynamique est activé, la préemption est retardée jusqu'à ce que les connexions soient répliquées à partir de l'unité sur laquelle le groupe de basculement est actuellement actif.

Si vous basculez manuellement, la commande **preempt** est ignorée.

Étape 10 Créez le groupe de basculement 2 et affectez-le à l'unité secondaire :

failover group 2

secondary

preempt [*delay*]

Exemple :

```
ciscoasa(config-fover-group)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 1200
```

Étape 11 Entrez en mode de configuration de contexte pour un contexte donné et affectez le contexte à un groupe de basculement :

context *nom*

join-failover-group {**1** | **2**}

Exemple :

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

Répétez cette commande pour chaque contexte.

Toutes les contextes non affectés sont automatiquement affectés au groupe de basculement 1. Le contexte d'administration est toujours membre du groupe de basculement 1; vous ne pouvez pas l'affecter au groupe 2.

Étape 12 Activez le basculement :

failover

Étape 13 Enregistrez la configuration système dans la mémoire flash :

write memory

Exemples

L'exemple suivant configure les paramètres de basculement pour l'unité principale :

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4

failover interface ip statelink 172.27.48.2 255.255.255.254 standby 172.27.48.3
interface gigabitethernet 0/4
  no shutdown
failover group 1
  primary
  preempt
failover group 2
  secondary
  preempt
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

Configurer l'unité secondaire pour le basculement actif/actif

La seule configuration requise sur l'unité secondaire concerne la liaison de basculement. L'unité secondaire exige que ces commandes communiquent initialement avec l'unité principale. Une fois que l'unité principale a envoyé sa configuration à l'unité secondaire, la seule différence permanente entre les deux configurations est la commande **basculement LAN unité**, qui identifie chaque unité comme principale ou secondaire.

Avant de commencer

- Activez ou désactivez le mode de contexte multiple conformément à Activer ou désactiver le mode de contexte multiple, à la page 240.
- Vous ne pourrez pas activer le basculement si des interfaces sont configurées pour DHCP.
- Ne configurez pas d'argument **nameif** pour les liaisons de basculement et d'état.
- Effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Saisissez à nouveau les mêmes commandes que sur l'unité principale, *à l'exception* de la commande **basculement LAN unité principale**. Vous pouvez éventuellement la remplacer par la commande **basculement LAN unité secondaire**, mais ce n'est pas nécessaire, car **le paramètre secondaire** est le paramètre par défaut. Vous n'avez pas non plus besoin de saisir les commandes **failover group** et **join-failover-group**, car elles sont répliquées à partir de l'unité principale. Consultez Configurer l'unité principale pour le basculement actif/actif, à la page 304.

Par exemple :

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

Étape 2 Après la synchronisation de la configuration de basculement à partir de l'unité principale, enregistrez la configuration dans la mémoire flash :

ciscoasa(config)# **write memory**

Étape 3 Si nécessaire, forcez le groupe de basculement 2 à être actif sur l'unité secondaire :

failover active group 2

Configurer les paramètres de basculement facultatifs

Vous pouvez personnaliser les paramètres de basculement à votre guise.

Configurer les critères de basculement et les autres paramètres

Consultez Paramètres par défaut pour le basculement, à la page 299 pour connaître les paramètres par défaut pour de nombreux paramètres que vous pouvez modifier dans cette section. Pour le mode actif/actif, vous définissez la plupart des critères par groupe de basculement.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte multiple.

- Pour la détection de transfert bidirectionnel (BFD) des fonctions de surveillance de l'intégrité des unités, consultez les limites suivantes :
  - Firepower 9300 et 4100 uniquement.
  - Actif/Veille uniquement.
  - Mode routé uniquement

Procédure

Étape 1 Modifiez les délais d'interrogation et de rétention de l'unité :

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

Exemple :

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

La plage **polltime** est comprise entre 1 et 15 secondes ou entre 200 et 999 millisecondes. La plage **holdtime** est comprise entre 1 et 45 secondes ou entre 800 et 999 millisecondes. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à 3 fois le délai d'interrogation de l'unité. Grâce à un délai d'interrogration plus court, l'ASA peut détecter les défaillances et déclencher le basculement plus rapidement. Cependant, une détection plus rapide peut entraîner des basculements inutiles lorsque le réseau est temporairement congestionné.

Si une unité n'entend pas le paquet Hello sur l'interface de communication de basculement pendant une période d'interrogation, des tests supplémentaires sont effectués par les interfaces restantes. S'il n'y a toujours aucune réponse de l'unité homologue pendant le délai de rétention, l'unité est considérée comme défaillante et, si l'unité défaillante est l'unité active, l'unité en veille prend le relais en tant qu'unité active.

En mode actif/actif, vous définissez ce débit pour le système; vous ne pouvez pas définir ce débit par groupe de basculement.

Étape 2 Configurez la BFD pour la surveillance de l'intégrité de l'unité.

La surveillance régulière de l'unité peut déclencher de fausses alarmes lorsque l'utilisation du CPU est élevée. La méthode BFD est distribuée, de sorte qu'un CPU élevé n'affecte pas son fonctionnement.

a) Définissez un modèle de BFD à utiliser pour la détection de l'état de basculement :

bfd-template single-hop *template_name*

bfd interval min-tx *milliseconds***min-rx** *milliseconds* **multiplier** *multiplier_value*

Exemple :

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
```

Le **min-tx** spécifie le débit auquel les paquets de contrôle de la BFD sont envoyés à l'homologue de basculement. La plage va de 50 à 999 millisecondes. Le **min-rx** spécifie le débit auquel les paquets de contrôle de la BFD doivent être reçus de l'homologue de basculement. La plage va de 50 à 999 millisecondes. Le **multiplier** spécifie le nombre de paquets de contrôle BFD consécutifs qui doivent

être manqués par un homologue de basculement avant que la BFD ne déclare que l'homologue n'est pas disponible. La valeur doit être comprise entre 3 et 50.

Vous pouvez également configurer l'écho et l'authentification pour ce modèle; voir Créer le modèle BFD, à la page 993.

b) Activez la BFD pour la surveillance de l'intégrité :

failover health-check bfd *template_name*

Exemple :

```
ciscoasa(config)# failover health-check bfd failover-temp
```

Étape 3 Modifiez le délai d'interrogation sur l'état de la liaison d'interface :

failover polltime link-state msec *poll_time*

Exemple :

```
ciscoasa(config)# failover polltime link-state msec 300
```

La plage est comprise entre 300 et 799 millisecondes. Par défaut, chaque ASA d'une paire de basculement vérifie l'état de liaison de ses interfaces toutes les 500 ms. Vous pouvez personnaliser le délai d'interrogation. Par exemple, si vous définissez le délai d'interrogation à 300 ms, l'ASA peut détecter une défaillance d'interface et déclencher le basculement plus rapidement.

En mode actif/actif, vous définissez ce débit pour le système; vous ne pouvez pas définir ce débit par groupe de basculement.

Étape 4 Définissez le taux de réplication de session en connexions par seconde :

failover replication rate *conns*

Exemple :

```
ciscoasa(config)# failover replication rate 20000
```

Le débit minimum et maximum est déterminé par votre modèle. La valeur par défaut est le taux maximum. En mode actif/actif, vous définissez ce débit pour le système; vous ne pouvez pas définir ce débit par groupe de basculement.

Étape 5 Désactivez la possibilité d'apporter des modifications à la configuration directement sur l'unité ou le contexte en veille :

failover standby config-lock

Par défaut, les configurations sur l'unité/le contexte de veille sont autorisées avec un message d'avertissement.

Étape 6 (Mode actif/actif uniquement) Spécifiez le groupe de basculement que vous souhaitez personnaliser :

failover group {**1** | **2**}

Exemple :

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

Étape 7 Activez la réplication de l'état HTTP :

- Pour le mode actif/veille :

  failover replication http

- Pour le mode actif/actif :

  replication http

Pour permettre l'inclusion des connexions HTTP dans la réplication des renseignements d'état, il est nécessaire d'activer la réplication HTTP. Nous vous conseillons d'activer la réplication de l'état HTTP.

Remarque
En raison d'un retard lors de la suppression des flux HTTP de l'unité de secours lors de l'utilisation du basculement, la sortie **show conn count** pourrait afficher des numéros différents sur l'unité active par rapport à l'unité de secours; si vous attendez plusieurs secondes et réexécutez la commande, vous verrez le même nombre sur les deux unités.

Étape 8 Définissez le seuil de basculement lorsque les interfaces tombent en panne :

- Pour le mode actif/veille :

  failover interface-policy *num* [%]

  Exemple :

  ```
  ciscoasa (config)# failover interface-policy 20%
  ```

- Pour le mode actif/actif :

  interface-policy *num* [%]

  Exemple :

  ```
  ciscoasa(config-fover-group)# interface-policy 20%
  ```

Par défaut, la défaillance d'une interface entraîne le basculement.

Lorsque vous spécifiez un nombre spécifique d'interfaces, l'argument *num* peut être compris entre 1 et 1 025.

Lors de la spécification d'un pourcentage d'interfaces, l'argument *num* peut être compris entre 1 et 100.

Étape 9 Modifiez les délais d'interrogation et de rétention de l'interface :

- Pour le mode actif/veille :

  failover polltime interface [**msec**] *polltime* [**holdtime** *time*]

  Exemple :

  ```
  ciscoasa(config)# failover polltime interface msec 500 holdtime 5
  ```

- Pour le mode actif/actif :

  polltime interface [**msec**] *polltime* [**holdtime***time*]

  Exemple :

```
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
```

- *polltime* : définit la durée d'attente entre l'envoi d'un paquet Hello à l'homologue. Les valeurs valides pour le délai d'interrogation vont de 1 à 15 secondes ou, si le mot clé facultatif **msec** est utilisé, de 500 à 999 millisecondes. La valeur par défaut est de 5 secondes.
- **holdtime***time* : définit le temps (sous forme de calcul) entre le dernier message Hello reçu de l'unité homologue et le début des tests d'interface pour déterminer l'intégrité de l'interface. Il définit également la durée de chaque test d'interface comme délai d'attente/16. Les valeurs valides sont comprises entre 5 et 75 secondes. La valeur par défaut est de 5 fois le délai d'interrogation. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à cinq fois le délai d'interrogation.

  Pour calculer le temps avant le début des tests d'interface (y) :

  1. x = (*durée d'attente*/*durée d'interrogation*)/2, arrondi à l'entier le plus proche. (0,4 et moins sont arrondis à l'unité inférieure; 0,5 et plus sont arrondis à l'unité supérieure).
  2. y = x**durée d'interrogation*

  Par exemple, si vous utilisez la délai d'attente par défaut de 25 et le délai d'interrogation de 5, alors y = 15 secondes.

Étape 10 Configurez l'adresse MAC virtuelle d'une interface :

- Pour le mode actif/veille :

  failover mac address *phy_if active_mac standby_mac*

  Exemple :

```
ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

- Pour le mode actif/actif :

  mac address *phy_if active_mac standby_mac*

  Exemple :

```
ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

L'argument *phy_if* est le nom physique de l'interface, tel que gigabitethernet0/1.

Les arguments *active_mac* et *standby_mac* sont des adresses MAC au format H.H.H, où H est un chiffre hexadécimal de 16 bits. Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE serait saisie comme suit : 000C.F142.4CDE.

L'adresse *active_mac* est associée à l'adresse IP active de l'interface, et l'adresse *standby_mac* est associée à l'adresse IP en veille pour l'interface.

Vous pouvez également définir l'adresse MAC à l'aide d'autres commandes ou méthodes, mais nous vous conseillons d'utiliser une seule méthode. Si vous définissez l'adresse MAC à l'aide de plusieurs méthodes, l'adresse MAC utilisée dépend de nombreuses variables et peut ne pas être prédictible.

Utilisez la commande **show interface** pour afficher l'adresse MAC utilisée par une interface.

Étape 11 (Mode actif/actif uniquement) Répétez cette procédure pour l'autre groupe de basculement.

Configurer la supervision de l'interface

Par défaut, la supervision est activée sur toutes les interfaces physiques, ou pour le Firepower 1010, toutes les interfaces VLAN.Les ports de commutation Firepower 1010 ne sont pas admissibles à la surveillance d'interface.

Vous pourriez souhaiter empêcher les interfaces connectées à des réseaux moins critiques d'affecter votre politique de basculement.

Vous pouvez superviser jusqu'à 1 025 interfaces sur une unité (dans tous les contextes en mode de contexte multiple).

Avant de commencer

En mode de contexte multiple, configurez les interfaces dans chaque contexte.

Procédure

Activez ou désactivez la surveillance de l'intégrité pour une interface :

[**no**] **monitor-interface** {*if_name*}

Exemple :

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

Configurer la prise en charge des paquets routés asymétriques (mode actif/actif)

Lorsqu'elle fonctionne en mode de basculement actif/actif, une unité peut recevoir un paquet de retour pour une connexion provenant de son unité homologue. Comme l'ASA qui reçoit le paquet n'a aucune information de connexion pour le paquet, le paquet est abandonné. Cet abandon se produit le plus généralement lorsque les deux ASA d'une paire de basculement actif/actif sont connectés à des fournisseurs de services différents et que la connexion sortante n'utilise pas d'adresse NAT.

Vous pouvez empêcher l'abandon des paquets de retour en autorisant les paquets routés de manière asymétrique. Pour ce faire, vous attribuez les interfaces similaires sur chaque ASA au même groupe ASR. Par exemple, les deux ASA se connectent au réseau interne sur l'interface interne, mais se connectent à des fournisseurs de services Internet distincts sur l'interface externe. Sur l'unité principale, affectez le contexte actif externe à l'interface au groupe ASR 1; sur l'unité secondaire, affectez le contexte actif en dehors de l'interface au même groupe ASR 1. Lorsque l'unité principale externe reçoit un paquet pour lequel elle n'a aucune information de session, elle vérifie les renseignements de session pour les autres interfaces dans les contextes de veille

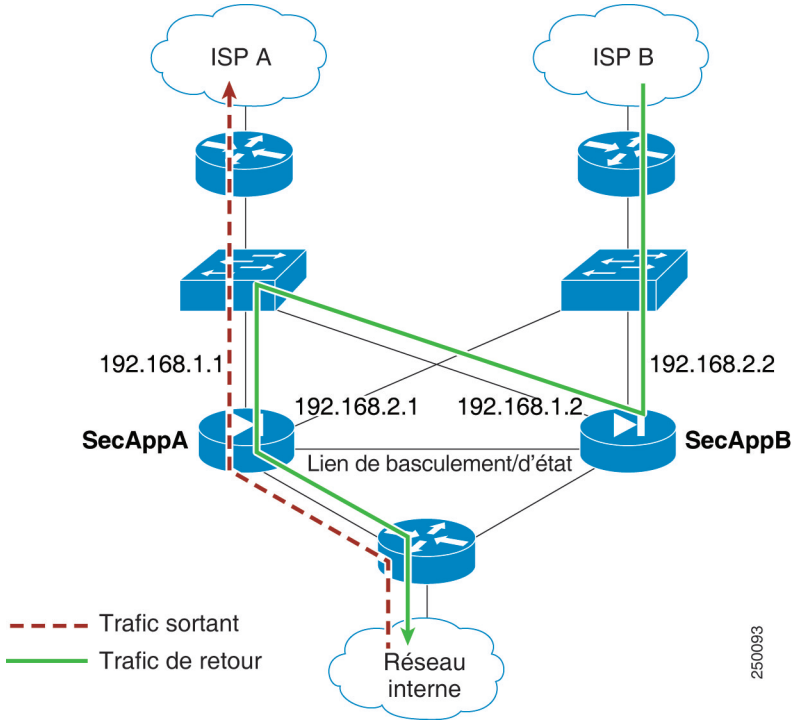
qui sont dans le même groupe; dans ce cas, le groupe ASR 1. Si elle ne trouve aucune correspondance, le paquet est abandonné. Si elle trouve une correspondance, l'une des actions suivantes se produit :

- Si le trafic entrant provient d'une unité homologue, tout ou partie de l'en-tête de couche 2 est réécrit et le paquet est redirigé vers l'autre unité. Cette redirection se poursuit tant que la session est active.
- Si le trafic entrant provient d'une interface différente sur la même unité, une partie ou la totalité de l'en-tête de couche 2 est réécrit et le paquet est réinjecté dans le flux.

Remarque Cette fonctionnalité ne fournit pas de routage asymétrique; elle restaure les paquets routés de manière asymétrique vers la bonne interface.

La figure suivante montre un exemple de paquet routé de manière asymétrique.

Illustration 48 : Exemple ASR



1. Une session sortante passe par l'ASA avec le contexte SecAppA actif. Elle quitte l'interface en dehors du FAI-A (192.168.1.1).
2. En raison d'un routage asymétrique configuré quelque part en amont, le trafic de retour passe par l'interface externe du FAI-B (192.168.2.2) sur l'ASA avec le contexte SecAppB actif.
3. Normalement, le trafic de retour serait abandonné, car il n'y a aucune information de session pour le trafic sur l'interface 192.168.2.2. Cependant, l'interface est configurée dans le cadre du groupe ASR 1. L'unité recherche la session sur toute autre interface configurée avec le même ID de groupe ASR.
4. Les renseignements de session se trouvent sur l'interface externe du FAI-A (192.168.1.2), qui est en état de veille sur l'unité avec SecAppB. Le basculement dynamique a répliqué les renseignements de session de SecAppA à SecAppB.

5. Au lieu d'être abandonné, l'en-tête de couche 2 est réécrit avec les renseignements pour l'interface 192.168.1.1 et le trafic est redirigé hors de l'interface 192.168.1.2, où il peut ensuite revenir par l'interface de l'unité à partir de laquelle il provient (192.168.1.1. sur SecAppA). Ce transfert se poursuit au besoin jusqu'à la fin de la session.

Avant de commencer

- Basculement dynamique : transmet les renseignements relatifs à l'état de session sur les interfaces du groupe de basculement actif au groupe de basculement de secours.
- HTTP de réplication : les renseignements relatifs à l'état de session HTTP ne sont pas transmis au groupe de basculement de secours et ne sont donc pas présents sur l'interface de secours. Pour que l'ASA puisse réacheminer les paquets HTTP routés de manière asymétrique, vous devez répliquer les renseignements relatifs à l'état HTTP.
- Effectuez cette procédure dans chaque contexte actif sur les unités principale et secondaire.
- Vous ne pouvez pas configurer à la fois des groupes ASR et des zones de trafic dans un contexte. Si vous configurez une zone dans un contexte, aucune des interfaces de contexte ne peut faire partie d'un groupe ASR.

Procédure

Étape 1 Sur l'unité principale, spécifiez l'interface pour laquelle vous souhaitez autoriser les paquets routés de manière asymétrique :

interface *phy_if*

Exemple :

```
primary/admin(config)# interface gigabitethernet 0/0
```

Étape 2 Définissez le numéro de groupe ASR de l'interface :

asr-group *num*

Exemple :

```
primary/admin(config-ifc)# asr-group 1
```

Les valeurs valides pour *num* vont de 1 à 32.

Étape 3 Sur l'unité secondaire, spécifiez l'interface similaire pour laquelle vous souhaitez autoriser les paquets routés de manière asymétrique :

interface *phy_if*

Exemple :

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

Étape 4 Définissez le numéro de groupe ASR de l'interface pour qu'il corresponde à l'interface de l'unité principale :

asr-group *num*

Exemple :

```
secondary/ctx1(config-ifc)# asr-group 1
```

Exemples

Les deux unités ont la configuration suivante (les configurations affichent seulement les commandes pertinentes). Le périphérique étiqueté SecAppA dans le diagramme est l'unité principale de la paire de basculement.

Configuration système de l'unité principale

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

Configuration du contexte SecAppA

```
interface GigabitEthernet0/2
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
```

```
monitor-interface outside
```

Configuration du contexte SecAppB

```
interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

Gérer Failover (basculement)

Cette section décrit comment gérer les unités Failover (basculement) après avoir activé Failover (basculement), y compris comment modifier la configuration Failover (basculement) et comment forcer le basculement d'une unité à une autre.

Forcer le basculement

Pour forcer l'unité en veille à devenir active, procédez comme suit.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Forcez un basculement lorsque vous avez saisi la commande sur l'unité *en veille*. L'unité en veille devient l'unité active.

Si vous spécifiez le **groupe** *group_id*, cette commande force un basculement lorsqu'elle est saisie sur l'unité *en veille* pour le groupe de basculement actif/actif spécifié. L'unité en veille devient l'unité active du groupe de basculement.

- Pour le mode actif/veille sur l'unité en veille :

  failover active

- Pour le mode actif/actif sur l'unité en veille :

  failover active [**group** *group_id*]

  Exemple :

  ```
  standby# failover active group 1
  ```

Étape 2 Forcez un basculement lorsque vous avez saisi la commande sur l'unité *active*. L'unité active devient l'unité en veille.

Si vous spécifiez le **groupe** *group_id*, cette commande force un basculement lorsqu'elle est saisie sur l'unité *active* pour le groupe de basculement spécifié. L'unité active devient l'unité en veille du groupe de basculement.

- Pour le mode actif/veille sur l'unité active :

  no failover active

- Pour le mode actif/actif sur l'unité active :

  no failover active [**group** *group_id*]

  Exemple :

```
active# no failover active group 1
```

Désactiver le basculement

La désactivation du basculement sur une ou les deux unités permet de maintenir l'état actif et de veille de chaque unité jusqu'à ce que vous rechargiez. Pour une paire de basculement actif/actif, les groupes de basculement restent à l'état actif sur l'unité où ils sont actifs, quelle que soit l'unité pour laquelle ils sont configurés en priorité.

Affichez les caractéristiques suivantes lorsque vous désactivez le basculement :

- L'unité ou le contexte en veille reste en mode veille pour que les deux unités ne commencent pas à transmettre du trafic (cela s'appelle un état de pseudo-veille).
- L'unité ou le contexte en veille continue d'utiliser ses adresses IP en veille même s'il n'est plus connecté à une unité ou un contexte actif.
- L'unité ou le contexte en veille continue d'écouter une connexion sur la liaison de basculement. Si le basculement est réactivé sur l'unité ou le contexte actif, l'unité ou le contexte en veille reprend son état de veille ordinaire après avoir resynchronisé le reste de sa configuration.
- N'activez pas le basculement manuellement sur l'unité en veille; consultez plutôt Forcer le basculement, à la page 319. Si vous activez le basculement sur l'unité en veille, vous verrez un conflit d'adresses MAC qui peut perturber le trafic IPv6.
- Pour vraiment désactiver le basculement, enregistrez la configuration sans basculement dans la configuration de démarrage, puis rechargez.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Désactivez le basculement :

no failover

Étape 2 Pour désactiver complètement le basculement, enregistrez la configuration et rechargez :

write memory

reload

Restaurer une unité défaillante

Pour restaurer une unité défaillante à un état sans échec, effectuez la procédure suivante.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Restaurez une unité défaillante à un état sans échec :

- Pour le mode actif/veille :

  failover reset

- Pour le mode actif/actif :

  failover reset [**group** *group_id*]

  Exemple :

```
ciscoasa(config)# failover reset group 1
```

La restauration d'une unité défaillante à un état sans échec ne la rend pas automatiquement active; les unités restaurées restent en état de veille jusqu'à ce qu'elles soient activées par le basculement (forcé ou naturel). Une exception est un groupe de basculement (mode actif/actif uniquement) configuré avec une préemption de basculement. S'il était précédemment actif, un groupe de basculement devient actif s'il est configuré avec la préemption et si l'unité sur laquelle il a échoué est l'unité préférée.

Si vous spécifiez le **groupe** *group_id*, cette commande restaure un groupe de basculement actif/actif défaillant à un état sans échec.

Étape 2 (Mode actif/actif uniquement) Pour réinitialiser le basculement au niveau du groupe de basculement :

a) Dans le système, choisissez **Monitoring (Supervision) > Failover (Basculement) > Failover Group (Groupe de basculement)#**, où # correspond au numéro du groupe de basculement que vous souhaitez contrôler.

b) Cliquez sur **Reset Basculement** (Réinitialiser le basculement).

Resynchroniser la configuration

Si vous saisissez la commande write standby sur l'unité active, l'unité en veille efface sa configuration en cours d'exécution (à l'exception des commandes de basculement utilisées pour communiquer avec l'unité active) et l'unité active envoie sa configuration complète à l'unité en veille.

Pour le mode de contexte multiple, lorsque vous saisissez la commande **write standby** dans l'espace d'exécution du système, tous les contextes sont répliqués. Si vous saisissez la commande **write standby** dans un contexte, la commande ne réplique que la configuration du contexte.

Les commandes répliquées sont stockées dans la configuration en cours d'exécution.

Tester la fonctionnalité de basculement

Pour tester la fonctionnalité de basculement, effectuez la procédure suivante.

Procédure

Étape 1 Vérifiez que votre unité active transmet le trafic comme prévu à l'aide du protocole FTP (par exemple) pour envoyer un fichier entre des hôtes sur différentes interfaces.

Étape 2 Forcez un basculement en saisissez la commande suivante sur l'unité active :

Mode actif/veille

ciscoasa(config)# **no failover active**

Mode actif/actif

ciscoasa(config)# **no failover active group** *group_id*

Étape 3 Utilisez FTP pour envoyer un autre fichier entre les deux mêmes hôtes.

Étape 4 Si le test a échoué, saisissez la commande **show failover** pour vérifier l'état du basculement.

Étape 5 Lorsque vous avez terminé, vous pouvez rétablir l'état actif de l'unité en saisissant la commande suivante sur l'unité nouvellement active :

Mode actif/veille

ciscoasa(config)# **no failover active**

Mode actif/actif

ciscoasa(config)# **failover active group** *group_id*

Remarque
Lorsqu'une interface ASA tombe en panne, le basculement est toujours considéré comme un problème d'unité. Si l'ASA détecte qu'une interface est en panne, le basculement se produit immédiatement, sans attendre le délai de rétention de l'interface. Le délai de rétention de l'interface n'est utile que lorsque l'ASA considère que son état est OK, bien qu'il ne reçoive pas de paquets Hello de l'homologue. Pour simuler le délai de rétention de l'interface, fermez le réseau VLAN sur le commutateur pour empêcher les homologues de recevoir des paquets Hello les uns des autres.

Exécution de la commande à distance

L'exécution de commandes à distance vous permet d'envoyer des commandes saisies dans la ligne de commande à un homologue de basculement donné.

Envoyer une commande

Étant donné que les commandes de configuration sont répliquées de l'unité ou du contexte actif vers l'unité ou le contexte en veille, vous pouvez utiliser la commande **failover exec** pour saisir des commandes de configuration sur l'unité appropriée, quelle que soit l'unité à laquelle vous êtes connecté. Par exemple, si vous êtes connecté à l'unité en veille, vous pouvez utiliser la commande **failover exec active** pour envoyer les modifications de configuration à l'unité active. Ces modifications sont ensuite répliquées sur l'unité en veille. N'utilisez pas la commande **failover exec** pour envoyer des commandes de configuration à l'unité ou au contexte en veille; ces modifications de configuration ne sont pas répliquées sur l'unité active et les deux configurations ne seront plus synchronisées.

La sortie des commandes de configuration, d'exécution et **show** est affichée dans la session de terminal actuelle. Vous pouvez donc utiliser la commande **failover exec** pour émettre des commandes **show** sur une unité homologue et afficher les résultats dans le terminal actuel.

Vous devez disposer des privilèges suffisants pour exécuter une commande sur l'unité locale afin d'exécuter la commande sur l'unité homologue.

Procédure

Étape 1 Si vous êtes en mode de contexte multiple, utilisez la commande **changeto context***name* pour passer au contexte que vous souhaitez configurer. Vous ne pouvez pas modifier les contextes sur l'homologue de basculement avec la commande **failover exec**.

Étape 2 Utilisez la commande suivante pour envoyer des commandes à l'unité de basculement spécifiée :

ciscoasa(config)# **failover exec** {**active** | **mate** | **standby**}

Utilisez le mot clé **active** ou **standby** pour que la commande soit exécutée sur l'unité spécifiée, même s'il s'agit de l'unité actuelle. Utilisez le mot clé **mate** pour que la commande soit exécutée sur l'homologue de basculement.

Les commandes qui provoquent un changement de mode de commande ne modifient pas l'invite de la session en cours. Vous devez utiliser la commande **show failover exec** pour afficher le mode de commande dans lequel la commande est exécutée. Consultez la section Modifier les modes de commande, page 7-53 pour en savoir plus.

Modifier les modes de commande

La commande **failover exec** conserve un état de mode de commande distinct du mode de commande de votre session de terminal. Par défaut, le mode de commande **failover exec** démarre en mode de configuration globale pour le périphérique indiqué. Vous pouvez modifier ce mode de commande en envoyant la commande appropriée (comme la commande **interface**) à l'aide de la commande **failover exec**. L'invite de session ne change pas lorsque vous changez de mode à l'aide de **failover exec**.

Par exemple, si vous êtes connecté au mode de configuration globale de l'unité active d'une paire de basculement et que vous utilisez la commande **failover exec active** pour passer en mode de configuration d'interface, l'invite du terminal reste en mode de configuration globale, mais les commandes saisies à l'aide de **failover exec** sont saisies en mode de configuration d'interface.

Les exemples suivants montrent la différence entre le mode de session de terminal et le mode de commande **failover exec**. Dans l'exemple, l'administrateur change le mode **failover exec** sur l'unité active au mode de configuration d'interface pour l'interface GigabitEthernet0/1. Après cela, toutes les commandes saisies à l'aide de **failover exec active** sont envoyées au mode de configuration d'interface pour l'interface GigabitEthernet0/1. L'administrateur utilise ensuite l'exécution du basculement pour attribuer une adresse IP à cette interface. Bien que l'invite indique le mode de configuration globale, le mode **failover exec active** est en mode de configuration d'interface.

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
ciscoasa(config)# router rip
ciscoasa(config-router)#
```

La modification des modes de commande pour votre session actuelle avec le périphérique n'affecte pas le mode de commande utilisé par la commande **failover exec**. Par exemple, si vous êtes en mode de configuration d'interface sur l'unité active et que vous n'avez pas modifié le mode de commande **failover exec**, la commande suivante sera exécutée en mode de configuration globale. Il en résulte que votre session avec le périphérique reste en mode de configuration d'interface, tandis que les commandes saisies à l'aide de **failover exec active** sont envoyées en mode de configuration de routeur pour le processus de routage indiqué.

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

Utilisez la commande **show failover exec** pour afficher le mode de commande sur le périphérique indiqué dans lequel les commandes envoyées avec la commande **failover exec** sont exécutées. La commande **show failover exec** prend les mêmes mots clés que la commande **failover exec** : **active**, **mate** ou **standby**. Le mode **failover exec** pour chaque périphérique est suivi séparément.

Par exemple, voici une sortie de la commande **show failover exec** saisie sur l'unité de secours :

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode

ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

Questions de sécurité

La commande **failover exec** utilise la liaison de basculement pour envoyer des commandes à l'unité homologue et recevoir la sortie de l'exécution de la commande. Vous devez activer le chiffrement sur la liaison de basculement pour éviter les attaques clandestines ou d'intermittence.

Limites de l'exécution de la commande à distance

Lorsque vous utilisez des commandes à distance, vous êtes soumis aux limites suivantes :

- Si vous mettez à niveau une unité en utilisant la procédure de mise à niveau sans temps d'arrêt et pas l'autre, les deux unités doivent exécuter un logiciel qui prend en charge la commande **failover exec**.
- L'aide à l'exécution des commandes et au contexte n'est pas disponible pour les commandes dans l'argument *cmd_string*.
- En mode de contexte multiple, vous pouvez seulement envoyer des commandes au contexte homologue sur l'unité homologue. Pour envoyer des commandes à un contexte différent, vous devez d'abord passer à ce contexte sur l'unité à laquelle vous êtes connecté.
- Vous ne pouvez pas utiliser les commandes suivantes avec la commande **failover exec** :
  - **changeto**
  - **debug** (**undebug**)
- Si l'unité en veille est en état d'échec, elle peut toujours recevoir des commandes de la commande **failover exec** si la défaillance est causée par une défaillance de la carte de service; dans le cas contraire, l'exécution de la commande à distance échouera.
- Vous ne pouvez pas utiliser la commande **failover exec** pour passer du mode d'exécution privilégié au mode de configuration globale sur l'homologue de basculement. Par exemple, si l'unité actuelle est en mode d'exécution privilégié et que vous saisissez **failover exec mate configure terminal**, la sortie **show failover exec mate** affichera que la session d'exécution de basculement est en mode de configuration globale. Cependant, la saisie des commandes de configuration pour l'unité homologue à l'aide de **failover exec** échouera jusqu'à ce que vous passiez en mode de configuration globale sur l'unité actuelle.
- Vous ne pouvez pas saisir des commandes d'exécution de basculement récursives, telles que la commande **failover exec mate failover exec mate**.
- Les commandes qui nécessitent une entrée ou une confirmation de l'utilisateur doivent utiliser l'option **noconfirm**. Par exemple, pour recharger le partenaire, saisissez :

  failover exec mate reload noconfirm

Surveillance de Failover (basculement)

Cette section vous permet de surveiller l'état de Failover (basculement).

Messages de basculement

Lorsqu'un basculement se produit, les deux ASA envoient des messages système.

Messages de journal système de basculement

L'ASA émet un certain nombre de messages de journal système liés au basculement au niveau de priorité 2, ce qui indique une condition critique. Pour afficher ces messages, consultez le guide des messages du journal système. Les plages d'identifiants de message associés au basculement sont les suivantes : 101xxx, 102xxx,

103xxx, 104xxx, 105xxx, 210xxx, 311xxx, 709xxx et 727xxx. Par exemple, 105032 et 105043 indiquent un problème avec la liaison de basculement.

Remarque Pendant le basculement, l'ASA s'éteint de manière logique, puis affiche des interfaces, générant les messages de journal système 411001 et 411002. Il s'agit d'une activité normale.

Messages de débogage de basculement

Pour afficher les messages de débogage, saisissez la commande **debug fover**. Consultez la référence de commande pour en savoir plus.

Remarque Étant donné que la sortie de débogage se voit attribuer une priorité élevée dans le processus du CPU, elle peut affecter considérablement les performances du système. Par conséquent, les commandes **debug fover** doivent uniquement être utilisées pour résoudre des problèmes spécifiques ou au cours de sessions de dépannage effectuées avec le TAC de Cisco.

Interruptions de basculement SNMP

Pour recevoir des alertes SNMP de journal système pour le basculement, configurez l'agent SNMP pour envoyer des alertes SNMP aux stations de gestion SNMP, définissez un hôte de journal système et compilez la MIB de journal système Cisco dans votre station de gestion SNMP.

Supervision de l'état du basculement

Pour superviser l'état du basculement, saisissez l'une des commandes suivantes :

- **afficher le basculement**

  Affiche des renseignements sur l'état de basculement de l'unité.

- **show failover group**

  Affiche des renseignements sur l'état de basculement du groupe de basculement. Les renseignements affichés sont similaires à ceux de la commande **show failover**, mais limités au groupe spécifié.

- **show monitor-interface**

  Affiche des renseignements sur l'interface supervisée.

- **show running-config failover**

  Affiche les commandes de basculement dans la configuration en cours d'exécutionn.

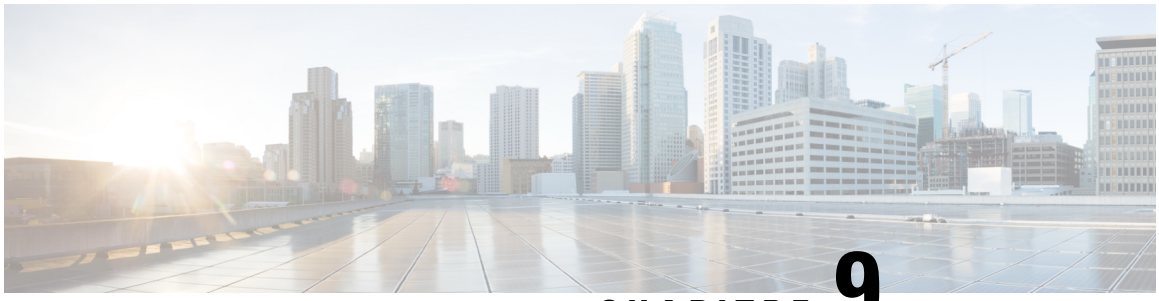
Historique de basculement

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement actif/de secours	7.0(1)	Cette fonctionnalité a été introduite.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement actif/actif	7.0(1)	Cette fonctionnalité a été introduite.
Prise en charge d'une valeur hexadécimale pour la clé de basculement	7.0(4)	Vous pouvez maintenant spécifier une valeur hexadécimale pour le chiffrement de la liaison de basculement. Nous avons modifié la commande suivante : **failover key hex**.
Prise en charge de la phrase secrète principale pour la clé de basculement	8.3(1)	La clé de basculement prend désormais en charge la phrase secrète principale, qui chiffre la clé partagée dans la configuration de démarrage. Si vous copiez le secret partagé d'un ASA à un autre, par exemple à partir de la commande **more system:running-config**, vous pouvez copier et coller la clé partagée chiffrée avec succès. **Remarque** Le secret partagé **failover key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée. Nous avons modifié la commande suivante : **failover key** [**0** | **8**].
Ajout de la prise en charge d'IPv6 pour le basculement.	8.2(2)	Nous avons modifié les commandes suivantes : **failover interface ip**, **show failover**, **ipv6 address**, **show monitor-interface**.
Modifiez la préférence de l'unité de groupe de basculement lors du démarrage « simultané ».	9.0(1)	Les versions logicielles antérieures permettaient un démarrage « simultané » de sorte que les groupes de basculement ne devaient pas exiger que la commande **preempt** devienne active sur l'unité préférée. Cependant, cette fonctionnalité a maintenant été modifiée, de sorte que les deux groupes de basculement deviennent actifs sur la première unité de démarrage.
Prise en charge des tunnels IPsec LAN à LAN pour chiffrer les communications de liaison de basculement et d'état	9.1(2)	Au lieu d'utiliser le chiffrement propriétaire pour la clé de basculement (la commande **failover key**), vous pouvez désormais utiliser un tunnel IPsec LAN à LAN pour le chiffrement de la liaison de basculement et d'état. **Remarque** Les tunnels de basculement LAN à LAN ne sont pas pris en compte dans la licence IPsec (autre VPN). Nous avons introduit ou modifié les commandes suivantes : **failover ipsec pre-shared-key**, **show vpn-sessiondb**.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Désactiver la surveillance de l'intégrité d'un module matériel	9.3(1)	Par défaut, l'ASA surveille l'intégrité d'un module matériel installé tel que le module ASA FirePOWER. Si vous ne souhaitez pas qu'une défaillance du module matériel déclenche le basculement, vous pouvez désactiver la surveillance du module. Nous avons modifié la commande suivante : **monitor-interface service-module**
Verrouiller les modifications de configuration sur l'unité de veille ou le contexte de veille dans une paire de basculement	9.3(2)	Vous pouvez désormais verrouiller les modifications de configuration sur l'unité de veille (basculement actif/veille) ou sur le contexte de veille (basculement actif/actif) afin de ne pas pouvoir apporter des modifications sur l'unité de veille en dehors de la synchronisation normale de la configuration. Nous avons introduit la commande suivante : **failover standby config-lock**
Activer l'utilisation de l'interface de gestion Management 1/1 comme liaison de basculement sur l'ASA 5506H	9.5(1)	Sur l'ASA 5506H uniquement, vous pouvez maintenant configurer l'interface de gestion Management 1/1 comme liaison de basculement. Cette fonctionnalité vous permet d'utiliser toutes les autres interfaces du périphérique comme interfaces de données. Notez que si vous utilisez cette fonctionnalité, vous ne pouvez pas utiliser le module ASA Firepower, ce qui nécessite que l'interface de gestion Management 1/1 reste une interface de gestion normale. Nous avons modifié les commandes suivantes : **failover lan interface, failover link**
Les améliorations de la NAT de classe opérateur sont désormais prises en charge dans le basculement et la mise en grappe d'ASA	9.5(2)	Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Cette fonctionnalité est désormais prise en charge dans les déploiements de basculement et de grappe ASA. Nous avons modifié la commande suivante : **show local-host**
Temps de synchronisation amélioré pour les ACL dynamiques de Secure Client (services client sécurisés) lors de l'utilisation du basculement actif/veille	9.6(2)	Lorsque vous utilisez Secure Client (services client sécurisés) sur une paire de basculement, le temps de synchronisation des ACL dynamiques (dACLs) associées avec l'unité de veille est maintenant amélioré. Auparavant, avec de grandes dACLs, le temps de synchronisation pouvait prendre des heures pendant lesquelles l'unité de veille était occupée à synchroniser au lieu de fournir une sauvegarde à haute disponibilité. Nous n'avons pas modifié de commandes.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement avec état pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple	9.6(2)	Le basculement avec état est maintenant pris en charge pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple. Nous n'avons pas modifié de commandes.
L'interrogation de la surveillance de l'état de la liaison de l'interface pour le basculement est désormais configurable pour une détection plus rapide	9.7(1)	Par défaut, chaque ASA d'une paire de basculement vérifie l'état de liaison de ses interfaces toutes les 500 ms. Vous pouvez maintenant configurer l'intervalle entre interrogations, entre 300 ms et 799 ms; par exemple, si vous définissez le délai d'interrogation à 300 ms, l'ASA peut détecter une défaillance d'interface et déclencher le basculement plus rapidement. Nous avons introduit la commande suivante : **failover polltime link-state**
Prise en charge de la détection de transfert bidirectionnel (BFD) pour la surveillance de l'intégrité du basculement actif/veille sur les périphériques Firepower 9300 et 4100.	9.7(1)	Vous pouvez activer la détection de transfert bidirectionnel (BFD) pour la vérification de l'intégrité du basculement entre deux unités d'une paire active/veille sur les périphériques Firepower 9300 et 4100. L'utilisation de la BFD pour la vérification de l'intégrité est plus fiable que la méthode de vérification de l'intégrité par défaut et utilise moins de CPU. Nous avons introduit la commande suivante : **failover health-check bfd**
Désactiver le délai de basculement	9.15(1)	Lorsque vous utilisez des groupes de ponts ou DAD IPv6, lorsqu'un basculement se produit, la nouvelle unité active attend jusqu'à 3 000 ms que l'unité de veille termine les tâches de mise en réseau et passe à l'état de veille. Ensuite, l'unité active peut commencer à transmettre du trafic. Pour éviter ce délai, vous pouvez désactiver le délai d'attente afin que l'unité active commence à transmettre le trafic avant l'unité de veille. Commandes nouvelles ou modifiées : **failover wait-disable**
Fonction d'optimisation Config-Sync pour un appairage haute disponibilité	9.18(1)	La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration de l'unité qui rejoint l'unité et de l'unité active en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les unités actives et en cours de jonction correspond, l'unité à joindre ignore la configuration de synchronisation complète et rejoint la haute disponibilité. Cette fonctionnalité accélère l'appairage à haute disponibilité et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.



CHAPITRE 9

Basculement pour la haute disponibilité dans le nuage public

Ce chapitre décrit comment configurer le basculement actif/de secours pour atteindre la haute disponibilité de ASA virtuel dans un environnement de nuage public, comme Microsoft Azure.

- À propos du basculement dans le nuage public, à la page 331
- Licences pour le basculement dans le nuage public, à la page 336
- Valeurs par défaut pour le basculement dans le nuage public, à la page 336
- À propos de l'ASA virtuel à haute disponibilité dans Microsoft Azure, à la page 337
- Configurer le basculement actif/de secours, à la page 340
- Configurer les paramètres de basculement facultatifs, à la page 342
- Activer le basculement actif/de secours, à la page 347
- Gérer le basculement dans le nuage public, à la page 349
- Superviser le basculement dans le nuage public, à la page 351
- Historique de basculement dans le nuage public, à la page 352

À propos du basculement dans le nuage public

Pour assurer la redondance, vous pouvez déployer l'ASA virtuel dans un environnement de nuage public dans une configuration active/de secours à haute accessibilité (HA). La haute accessibilité dans le nuage public met en œuvre une solution active/de secours sans état qui permet, en cas de défaillance de l'ASA virtuel actif, de déclencher un basculement automatique du système vers l'ASA virtuel de secours.

La liste suivante décrit les composants principaux de la solution de nuage public à haute disponibilité :

- **ASA virtuel actif** : l'ASA virtuel dans la paire à haute disponibilité qui est configuré pour gérer le trafic de pare-feu pour les homologues à haute disponibilité.
- **ASA virtuel en veille** : l'ASA virtuel dans la paire à haute disponibilité qui ne gère pas le trafic du pare-feu et prend le relais comme ASA virtuel actif en cas de défaillance d'un ASA virtuel actif. Il est appelé sauvegarde plutôt que de secours, car il ne prend pas l'identité de son homologue en cas de basculement.
- **Agent à haute disponibilité** : un processus allégé qui s'exécute sur l'ASA virtuel et détermine le rôle de haute disponibilité (actif/sauvegarde) d'un ASA virtuel, détecte les défaillances de son homologue à haute disponibilité et effectue les actions en fonction de son rôle de haute disponibilité.

Sur l'ASA physique et l'ASA virtuel en nuage non public, le système gère les conditions de basculement à l'aide de demandes ARP gratuites, dans lesquelles l'ASA de secours envoie une requête ARP gratuite indiquant qu'il est désormais associé aux adresses IP et MAC actives. La plupart des environnements de nuage public n'autorisent pas le trafic de diffusion de cette nature. Pour cette raison, une configuration à haute disponibilité dans le nuage public nécessite le redémarrage des connexions permanentes lors du basculement.

L'intégrité de l'unité active est surveillée par l'unité de secours pour déterminer si des conditions de basculement spécifiques sont remplies. Si ces conditions sont remplies, le basculement se produit. Le délai de basculement peut varier de quelques secondes à plus d'une minute selon la réactivité de l'infrastructure de nuage public.

À propos du basculement actif/de secours

Dans le basculement actif/sauvegarde, une unité est l'unité active. Elle transmet le trafic. L'unité de sauvegarde ne transmet pas activement le trafic et n'échange aucune information de configuration avec l'unité active. Le basculement actif/de sauvegarde vous permet d'utiliser un périphérique ASA virtuel de sauvegarde pour reprendre les fonctionnalités d'une unité en panne. Lorsque l'unité active tombe en panne, elle passe à l'état de sauvegarde pendant que l'unité de sauvegarde passe à l'état actif.

Rôles principal/secondaire et état actif/de secours

Lors de la configuration du basculement actif/de sauvegarde, vous configurez une unité comme principale et l'autre comme secondaire. À ce stade, les deux unités agissent comme deux périphériques distincts pour la configuration des périphériques et des politiques, ainsi que pour les événements, les tableaux de bord, les rapports et la surveillance de l'intégrité.

Les principales différences entre les deux unités d'une paire de basculement dépendent de l'unité active et de l'unité de sauvegarde, à savoir l'unité qui transmet activement le trafic. Bien que les deux unités soient capables de transmettre du trafic, seule l'unité principale répond aux sondes de l'équilibreur de charges et programme toutes les routes configurées pour l'utiliser comme destination de routage. La fonction principale de l'unité de sauvegarde est de surveiller l'intégrité de l'unité principale. L'unité principale devient toujours l'unité active si les deux unités démarrent en même temps (et ont le même état de fonctionnement opérationnel).

Connexion de basculement

L'ASA virtuel de secours surveille l'intégrité de l'ASA virtuel actif à l'aide d'une connexion de basculement établie sur TCP :

- L'ASA virtuel actif agit comme un serveur de connexion en ouvrant un *port d'écoute*.
- L'ASA virtuel de secours se connecte à l'ASA virtuel actif à l'aide du *port de connexion*.
- En général, le *port d'écoute* et le *port de connexion* sont identiques, sauf si votre configuration requiert une traduction d'adresses réseau entre les unités ASA virtuel.

L'état de la connexion de basculement détecte la défaillance de l'ASA virtuelactif. Lorsque l'ASA virtuel de secours voit la connexion de basculement établie, il considère l'ASA virtuel actif comme *ayant échoué*. De même, si l'ASA virtuel de secours ne reçoit pas de réponse à un message keepalive envoyé à l'unité active, il considère l'ASA virtuel actif comme *ayant échoué*.

Thèmes connexes

Messages de sondage et Hello

L'ASA virtuel de secours envoie des messages Hello via la connexion de basculement à l'ASA virtuel actif et attend une réponse Hello en retour. La synchronisation des messages utilise un intervalle entre les interrogations, la période entre la réception d'une réponse Hello par l'unité ASA virtuel de secours et l'envoi du message Hello suivant. La réception de la réponse est imposée par un délai d'expiration de réception, appelé délai de rétention. Si la réception de la réponse Hello expire, l'ASA virtuel actif est considéré comme ayant échoué.

Les intervalles d'interrogation et de délai de rétention sont des paramètres configurables; voir Configurer les critères de basculement et les autres paramètres, à la page 342.

Détermination de l'unité active au démarrage

L'unité active est déterminée par les éléments suivants :

- Si une unité démarre et détecte un homologue qui fonctionne déjà comme actif, elle devient l'unité de sauvegarde.
- Si une unité démarre et ne détecte pas d'homologue, elle devient l'unité active.
- Si les deux unités démarrent simultanément, l'unité principale devient l'unité active et l'unité secondaire devient l'unité de sauvegarde.

Événements de basculement

Dans le cas d'un basculement actif/de secours, le basculement se produit de manière unitaire. Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque défaillance, le tableau indique la politique de basculement (basculement ou absence de basculement), l'action prise par l'unité active, l'action entreprise par l'unité de sauvegarde, et toute remarque spéciale sur la condition et les actions de basculement.

Tableau 17 : Événements de basculement

Défaillance	Politique	Action active	Action de sauvegarde	Notes
L'unité de sauvegarde voit une connexion de basculement se fermer	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante	Il s'agit du scénario de basculement standard.
L'unité active voit une connexion de basculement se fermer	Aucun basculement	Marquer la sauvegarde comme ayant échoué	S.O.	Le basculement vers une unité inactive ne doit jamais se produire.

Défaillance	Politique	Action active	Action de sauvegarde	Notes
L'unité active voit un délai d'expiration TCP sur la liaison de basculement	Aucun basculement	Marquer la sauvegarde comme ayant échoué	Aucune action	Le basculement ne doit pas se produire si l'unité active ne reçoit pas de réponse de l'unité de sauvegarde.
L'unité de sauvegarde voit un délai d'expiration TCP sur la liaison de basculement	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante Essayer d'envoyer la commande de basculement à l'unité active	L'unité de sauvegarde suppose que l'unité active n'est pas en mesure de continuer à fonctionner et prend le relais. Si l'unité active est toujours opérationnelle, mais n'envoie pas de réponse à temps, l'unité de sauvegarde envoie la commande de basculement à l'unité active.
Échec de l'authentification de l'unité active	Aucun basculement	Aucune action	Aucune action	Comme l'unité de sauvegarde modifie les tables de routage, c'est la seule unité qui doit être authentifiée auprès d'Azure. Peu importe si l'unité active est authentifiée auprès d'Azure ou non.
Échec de l'authentification de l'unité de sauvegarde	Aucun basculement	Marquer la sauvegarde comme non authentifiée	Aucune action	Le basculement ne peut pas se produire si l'unité de sauvegarde n'est pas authentifiée auprès d'Azure.
L'unité active lance le basculement intentionnel	Basculement	Devenir une sauvegarde	Devenir active	L'unité active lance le basculement en ferme la connexion de liaison de basculement. L'unité de sauvegarde voit la connexion se terminer et devient l'unité active.
L'unité de sauvegarde lance le basculement intentionnel	Basculement	Devenir une sauvegarde	Devenir active	L'unité de sauvegarde lance le basculement en envoyant un message de basculement à l'unité active. Lorsque l'unité active voit le message, elle ferme la connexion et devient l'unité de sauvegarde. L'unité de sauvegarde voit la connexion se terminer et devient l'unité active.

Défaillance	Politique	Action active	Action de sauvegarde	Notes
L'unité précédemment active récupère	Aucun basculement	Devenir une sauvegarde	Marquer le partenaire comme sauvegarde	Le basculement ne doit pas se produire, sauf si cela est absolument nécessaire.
L'unité active voit le message de basculement de l'unité de sauvegarde	Basculement	Devenir une sauvegarde	Devenir active	Peut se produire si un basculement manuel a été lancé par un utilisateur, ou si l'unité de sauvegarde a vu le délai d'expiration TCP, mais l'unité active est en mesure de recevoir des messages de l'unité de sauvegarde.

Lignes directrices et limites relatives à la licence

Cette section comprend les lignes directrices et les limites de cette fonctionnalité.

ASA virtuel Basculement pour la haute disponibilité dans le nuage public

Pour assurer la redondance, vous pouvez déployer l'ASA virtuel dans un environnement de nuage public dans une configuration active/de secours à haute accessibilité (HA).

- Pris en charge uniquement sur le nuage public Microsoft Azure; lors de la configuration de la machine virtuelle ASA virtuel, le nombre maximal de vCPU pris en charge est de 8; et la mémoire maximale prise en charge est de 64 Go de RAM. Consultez le Guide de démarrage d'ASA virtuel pour obtenir la liste complète des instances prises en charge.
- Met en œuvre une solution active/de secours sans état qui permet, en cas de défaillance de l'ASA virtuel actif, de déclencher un basculement automatique du système vers l'ASA virtuel de secours.

Restrictions

- Le basculement se fait de l'ordre des secondes plutôt que des millisecondes.
- La détermination du rôle à haute disponibilité et la capacité de participer en tant qu'unité à haute disponibilité dépendent de la connectivité TCP entre les homologues à haute disponibilité et entre une unité à haute disponibilité et l'infrastructure Azure. Il existe plusieurs situations où un ASA virtuel ne pourra pas participer en tant qu'unité à haute disponibilité :
  - L'incapacité à établir une connexion de basculement avec son homologue à haute disponibilité.
  - L'incapacité à récupérer un jeton d'authentification à partir d'Azure.
  - L'incapacité à s'authentifier auprès d'Azure.
- Il n'y a pas de synchronisation de la configuration de l'unité active avec l'unité de sauvegarde. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.
- Limites de la table de routage de basculement

En ce qui concerne les tables de routage pour la haute disponibilité dans le nuage public :

- Vous pouvez configurer un maximum de 16 tables de routage.
- Dans une table de routage, vous pouvez configurer un maximum de 64 routes.

Dans chaque cas, le système vous alerte lorsque vous avez atteint la limite, en vous recommandant de supprimer une table de routage ou une route et de réessayer.

- ASDM n'est pas pris en charge.
- Aucune prise en charge du VPN d'accès à distance IPSec.

Remarque Consultez le guide de démarrage rapide de Cisco Adaptive Security Virtual Appliance (ASAv) pour obtenir des renseignements sur les topologies VPN prises en charge dans le nuage public.

- Les instances de machine virtuelle ASA virtuel doivent se trouver dans le même ensemble de disponibilité. Si vous êtes un utilisateur ASA virtuel actuel dans Azure, vous ne pourrez pas effectuer de mise à niveau vers la haute disponibilité à partir d'un déploiement existant. Vous devez supprimer votre instance et déployer l'offre ASA virtuel 4 NIC à haute disponibilité depuis le Marché Azure.

Licences pour le basculement dans le nuage public

L'ASA virtuel utilise les licences logicielles Cisco Smart. Une licence Smart est requise pour le fonctionnement normal. Chaque ASA virtuel doit recevoir une licence indépendante avec une licence de plateforme ASA virtuel. Jusqu'à ce que vous installiez une licence, le débit est limité à 100 kbit/s. Vous pouvez donc effectuer des tests de connectivité préalables. Consultez la page Licences de fonctionnalités de la gamme Cisco ASA pour connaître les exigences de licence précises pour l'ASA virtuel.

Valeurs par défaut pour le basculement dans le nuage public

Par défaut, la politique de basculement comprend les éléments suivants :

- Basculement sans état uniquement.
- Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.
- Le numéro de port de contrôle de basculement TCP est 44442.
- Le numéro de port de la sonde d'intégrité de l'équilibreur de charges Azure est 44441.
- Le délai d'interrogation de l'unité est de 5 secondes.
- Le délai de rétention de l'unité est de 15 secondes.
- L'ASA virtuel répond aux sondes d'intégrité sur l'interface principale (Management 0/0).
- L'authentification ASA virtuel avec le principal de service Azure est effectuée sur l'interface principale (Management 0/0).

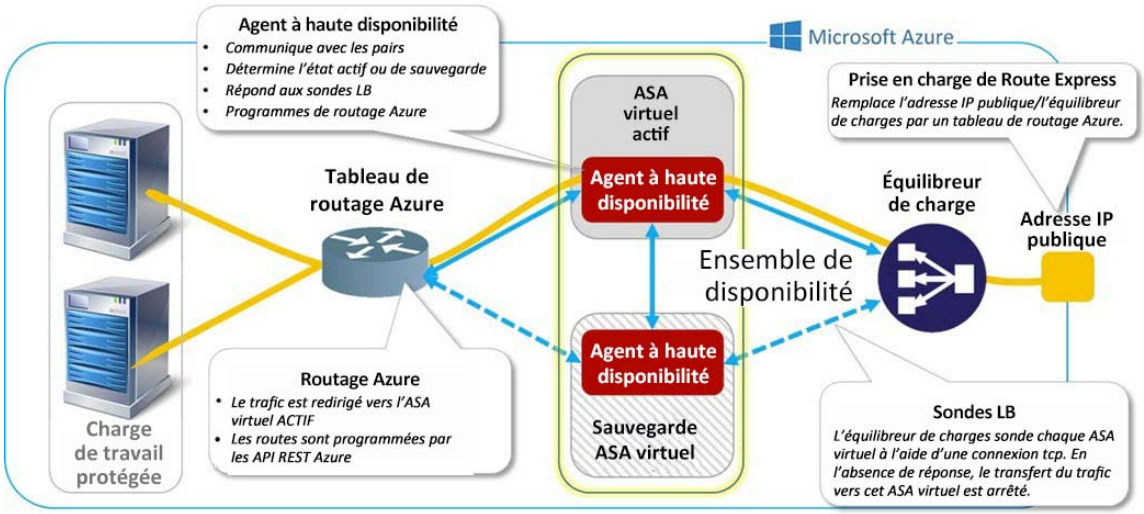
Remarque Consultez Configurer les paramètres de basculement facultatifs, à la page 342 pour connaître les options permettant de modifier le numéro de port de basculement, le numéro de port de la sonde d'intégrité, les délais d'interrogation et l'interface principale.

À propos de l'ASA virtuel à haute disponibilité dans Microsoft Azure

La figure suivante présente une vue d'ensemble d'un déploiement de l'ASA virtuel à haute disponibilité dans Azure. Une charge de travail protégée se trouve derrière deux instances ASA virtuel dans une configuration de basculement actif/de sauvegarde. Un équilibreur de charges Azure sonde les deux unités ASA virtuel à l'aide d'une liaison TCP tridirectionnelle. L'ASA virtuel actif termine l'établissement de la liaison tridirectionnelle indiquant qu'il est intègre, tandis que l'ASA virtuel de sauvegarde ne répond pas intentionnellement. En ne répondant pas à l'équilibreur de charges, l'ASA virtuel de sauvegarde semble non intègre à l'équilibreur de charges, qui à son tour, ne lui envoie pas de trafic.

Lors du basculement, l'ASA virtuel actif arrête de répondre aux sondes de l'équilibreur de charges et l'ASA virtuel de sauvegarde commence à répondre, ce qui fait que toutes les nouvelles connexions sont envoyées à l'ASA virtuel de sauvegarde. L'ASA virtuel de sauvegarde envoie des demandes API à la structure Azure pour modifier la table de routage, redirigeant ainsi le trafic de l'unité active vers l'unité de sauvegarde. À ce stade, l'ASA virtuel de sauvegarde devient l'unité active et l'unité active devient l'unité de sauvegarde ou est hors ligne, selon la raison du basculement.

Illustration 49 : Déploiement de l'ASA virtuel à haute disponibilité dans Azure



Pour pouvoir passer automatiquement des appels d'API pour modifier les tables de routage Azure, les unités ASA virtuel à haute disponibilité doivent disposer de renseignements d'authentification Azure Active Directory. Azure utilise le concept de principal de service qui, en termes simples, est un compte de service. Un principal de service vous permet de provisionner un compte avec seulement les autorisations et la portée nécessaires pour exécuter une tâche dans un ensemble prédéfini de ressources Azure.

Il y a deux étapes pour permettre à votre déploiement ASA virtuel à haute disponibilité de gérer votre abonnement Azure à l'aide d'un principal de service :

1. Créez une application Azure Active Directory et un principal de service; voir À propos du principal de service Azure, à la page 338.
2. Configurez les instances ASA virtuel pour s'authentifier auprès d'Azure à l'aide d'un principal de service; voir Configurer les informations d'authentification pour un principal de service Azure, à la page 344.

Thèmes connexes

Consultez la documentation d'Azure pour en savoir plus sur l'équilibreur de charges.

À propos du principal de service Azure

Lorsque vous avez une application qui a besoin d'accéder aux ressources d'Azure ou de les modifier, telles que des tables de routage, vous devez configurer une application Azure Active Directory (AD) et lui attribuer les autorisations requises. Il est préférable d'exécuter cette approche sous vos propres informations d'authentification, car :

- Vous pouvez attribuer des autorisations à l'identité de l'application qui sont différentes de vos propres autorisations. En règle générale, ces autorisations se limitent à ce que doit faire l'application.
- Vous n'avez pas besoin de modifier les informations d'authentification de l'application si vos responsabilités changent.
- Vous pouvez utiliser un certificat pour automatiser l'authentification lors de l'exécution d'un script sans surveillance.

Lorsque vous enregistrez une application Azure AD dans le portail Azure, deux objets sont créés dans votre détenteur Azure AD : un objet d'application et un objet de principal de service.

- **Application object** (Objet d'application) : une application Azure AD est définie par son seul et unique objet d'application, qui réside dans le détenteur Azure AD où l'application a été enregistrée, appelé détenteur « local » de l'application.
- **Service principal object** (Objet de principal de service) : l'objet de principal de service définit la politique et les autorisations pour l'utilisation d'une application dans un détenteur spécifique, fournissant la base d'un principal de sécurité pour représenter l'application lors de l'exécution.

Azure fournit des instructions sur la création d'une application et d'un principal de service Azure AD dans la *documentation d'Azure Resource Manager*. Consultez les rubriques suivantes pour obtenir des instructions complètes :

- Utiliser le portail pour créer une application et un principal de service Azure Active Directory qui peuvent accéder aux ressources
- Utiliser Azure PowerShell pour créer un principal de service pour accéder à la ressource

Remarque Après avoir configuré le principal de service, procurez-vous le **Directory ID** (ID de répertoire), l'**Application ID** (ID d'application) et la **Secret key** (Clé secrète). Ces éléments sont requis pour configurer les informations d'authentification Azure; voir Configurer les informations d'authentification pour un principal de service Azure, à la page 344.

Exigences de configuration pour ASA virtuel haute disponibilité dans Azure

Pour déployer une configuration similaire à celle décrite dans #unique_409 unique_409_Connect_42_fig_cgx_dlh_h1b, vous avez besoin des éléments suivants :

- Renseignements d'authentification Azure (voir À propos du principal de service Azure, à la page 338) :
  - ID de répertoire
  - ID d'application
  - Clé secrète
- Renseignements sur les routes Azure (voir Configurer les tableaux de routage Azure, à la page 345) :
  - ID d'abonnement Azure
  - Groupe de ressources de la table de routage
  - Noms de tables
  - Préfixe d'adresse
  - Adresse du saut suivant
- Configuration de l'ASA (voir Configurer le basculement actif/de secours, à la page 340, Valeurs par défaut pour le basculement dans le nuage public, à la page 336) :
  - Adresses IP actives ou de secours
  - Port de communication de l'agent à haute disponibilité
  - Port de sonde de l'équilibreur de charges
  - Intervalles entre interrogations

Remarque Configurez les paramètres de basculement de base sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.

Configurer le basculement actif/de secours

Pour configurer le basculement actif/de secours, configurez les paramètres de basculement de base sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.

Avant de commencer

- Déployez votre paire ASA virtuel à haute disponibilité dans un ensemble de disponibilité Azure.
- Ayez les renseignements sur votre environnement Azure à disposition, y compris votre ID d'abonnement Azure et vos informations d'authentification Azure pour le principal du service.

Configurer l'unité principale pour le basculement actif/de secours

Suivez les étapes de cette section pour configurer l'unité principale dans une configuration de basculement actif/de sauvegarde. Ces étapes fournissent la configuration minimum nécessaire pour activer le basculement sur l'unité principale.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.

Exemple

L'exemple suivant montre comment configurer les paramètres de basculement pour l'unité principale/active :

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(config)#
```

L'adresse IP homologue que vous saisissez ici doit être l'adresse IP de l'interface de gestion sur l'homologue à haute disponibilité de l'ASA virtuel.

Prochaine étape

Configurez les paramètres supplémentaires au besoin :

- Configurez l'unité de sauvegarde; voir Configurer l'unité secondaire pour le basculement actif/de secours, à la page 341.
- Configurez l'authentification Azure; voir Configurer les informations d'authentification pour un principal de service Azure, à la page 344.
- Configurez les renseignements sur les routes Azure; voir Configurer les tableaux de routage Azure, à la page 345.
- Passez en revue les paramètres supplémentaires; voir Configurer les critères de basculement et les autres paramètres, à la page 342.

Configurer l'unité secondaire pour le basculement actif/de secours

Suivez les étapes de cette section pour configurer l'unité secondaire dans une configuration de basculement actif/de secours. Ces étapes fournissent la configuration minimum nécessaire pour activer le basculement vers l'unité secondaire.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Étape 1 Désignez cette unité comme unité de secours :

failover cloud unit secondary

Étape 2 Attribuez l'adresse IP active à la liaison de basculement :

failover cloud peer ip *ip-address* [**port** *port-number*]

Cette adresse IP est utilisée pour établir une connexion de contrôle de basculement TCP avec l'homologue à haute disponibilité. Le port est utilisé lors de la tentative d'ouverture d'une connexion de basculement avec l'homologue à haute disponibilité, qui peut déjà être l'unité active. La configuration du port ici peut être nécessaire si la NAT est en place entre les homologues à haute disponibilité. Dans la plupart des cas, vous n'aurez pas besoin de configurer le port.

L'adresse IP homologue que vous saisissez ici doit être l'adresse IP de l'interface de gestion sur l'homologue à haute disponibilité de l'ASA virtuel.

Exemple

L'exemple suivant montre comment configurer les paramètres de basculement pour l'unité secondaire/de secours :

```
failover cloud unit secondary
failover cloud peer ip 10.4.3.4 port 4444
```

Prochaine étape

Configurez les paramètres supplémentaires au besoin :

- Configurez l'authentification Azure; voir Configurer les informations d'authentification pour un principal de service Azure, à la page 344.
- Configurez les renseignements sur les routes Azure; voir Configurer les tableaux de routage Azure, à la page 345.
- Passez en revue les paramètres supplémentaires; voir Configurer les critères de basculement et les autres paramètres, à la page 342.

Configurer les paramètres de basculement facultatifs

Vous pouvez personnaliser les paramètres de basculement selon vos besoins.

Configurer les critères de basculement et les autres paramètres

Consultez Valeurs par défaut pour le basculement dans le nuage public, à la page 336 pour connaître les paramètres par défaut pour de nombreux paramètres que vous pouvez modifier dans cette section.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.
- Configurez ces paramètres sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire.

Procédure

Étape 1 Spécifiez le port TCP à utiliser pour la communication avec l'homologue à haute disponibilité :

failover cloud port control *port-number*

Exemple :

```
ciscoasa(config)# failover cloud port control 4444
```

L'argument *port-number* attribue un numéro au port TCP utilisé pour la communication homologue à homologue.

Cela permet de configurer le port TCP de connexion de basculement sur lequel accepter les connexions lorsque l'unité est active. Il s'agit du port ouvert sur l'ASA virtuel actif auquel l'ASA virtuel de secours se connecte.

Remarque
Nous vous conseillons de conserver la valeur par défaut de 44442, qui est la valeur par défaut pour les deux homologues à haute disponibilité. Si vous modifiez la valeur par défaut d'un homologue à haute disponibilité, il est conseillé d'apporter la même modification à l'autre unité à haute disponibilité.

Étape 2 Modifiez les délais d'interrogation et de rétention de l'unité :

failover polltime *poll_time* [**holdtime** *time*]

Exemple :

```
ciscoasa(config)# failover polltime 10 holdtime 30
```

La plage **polltime** est comprise entre 1 et 15 secondes. Le délai de rétention détermine le délai entre le moment où un paquet Hello est manqué et le moment où l'unité est marquée comme défaillante. La plage **holdtime** est comprise entre 3 et 60 secondes. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à 3 fois le délai de sondage des unités. Grâce à un délai d'interrogration plus court, l'ASA peut détecter les

défaillances et déclencher le basculement plus rapidement. Cependant, une détection plus rapide peut entraîner des basculements inutiles lorsque le réseau est temporairement congestionné.

Étape 3 Spécifiez le port TCP utilisé pour les sondes d'intégrité de l'équilibreur de charges Azure :

failover cloud port probe *port-number*

Exemple :

```
ciscoasa(config)# failover cloud port probe 4443
```

Si votre déploiement utilise un équilibreur de charges Azure, l'ASA virtuel actif doit répondre aux sondes TCP de l'équilibreur de charges pour que les connexions entrantes soient dirigées vers l'unité active.

Étape 4 Spécifiez une interface secondaire pour les sondes d'intégrité de l'équilibreur de charges Azure :

failover cloud port probe *port-number* **interface** *if-name*

Exemple :

```
ciscoasa(config)# failover cloud port probe 4443 interface inside
```

Les sondes TCP utilisées dans le nuage à haute disponibilité ont l'adresse IP source de 168.63.129.16. Cette adresse est l'adresse IP publique virtuelle d'Azure. Cette adresse est l'adresse source des paquets DHCP Azure et est l'adresse du serveur de noms DNS dans Azure.

Par défaut, l'ASA virtuel répond aux sondes par lesquelles 168.63.129.16 est accessible, selon les tables de routage de l'ASA. Cela finit par être l'interface principale (Management0/0) en raison de la présence de la route par défaut.

Pour prendre en charge les équilibreurs de charges sur des interfaces autres que Management0/0, vous devez configurer une autre interface pour la sonde de port. Vous devez également configurer deux routes statiques : une pour l'interface principale et une pour l'interface configurée pour les sondes de l'équilibreur de charges.

Étape 5 Ajoutez des routes statiques pour l'interface principale et l'interface configurée pour les sondes de l'équilibreur de charges :

route *if-name dest_ip mask gateway_ip* **[distance]**

Exemple :

```
ciscoasa(config)# route outside 168.63.129.16 255.255.255.255 10.22.0.1 1
ciscoasa(config)# route inside 168.63.129.16 255.255.255.255 10.22.1.1 2
```

L'argument *distance* correspond à la distance administrative de la route. La valeur par défaut est **1** si vous ne spécifiez pas de valeur. La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. Lorsque plusieurs routes existent vers la même destination (168.63.129.16), la distance administrative de la route détermine la priorité.

La route statique de l'interface principale (extérieure) avec la distance administrative de 1 établit l'interface principale comme interface préférée pour les paquets destinés à 168.63.129.16, mais permet également à l'interface configurée pour les sondes de l'équilibreur de charges d'envoyer des paquets à 168.63.129.16.

Remarque
Le mécanisme de réponse aux sondes consiste à créer un connecteur TCP sur une interface. Le nuage à haute disponibilité utilise la recherche de routes pour 168.63.129.16 pour décider sur quelle interface créer le

connecteur. Cela finit par être l'interface principale en raison de la présence de la route par défaut. Sans la route statique de l'interface configurée pour les sondes, l'ASA ne répondrait pas aux paquets TCP envoyés par l'équilibreur de charges.

Configurer les informations d'authentification pour un principal de service Azure

Vous pouvez permettre à vos homologues à haute disponibilité ASA virtuel d'accéder aux ressources d'Azure, telles que des tables de routage, ou de modifier ces ressources à l'aide d'un principal de service Azure. Vous devez configurer une application Azure Active Directory (AD) et lui attribuer les autorisations requises. Les commandes suivantes permettent à l'ASA virtuel de s'authentifier auprès d'Azure à l'aide d'un principal de service. Consultez le chapitre Azure du guide de démarrage rapide d'ASA virtuel pour en savoir plus sur le principal de service Azure.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.
- Configurez ces paramètres sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire.

Procédure

Étape 1 Configurez l'ID d'abonnement Azure pour le principal de service Azure :

failover cloud subscription-id *subscription-id*

Exemple :

```
(config)# failover cloud subscription-id ab2fe6b2-c2bd-44
```

L'ID d'abonnement Azure est nécessaire pour modifier les tables de routage Azure, par exemple, lorsque l'utilisateur de haute disponibilité en nuage souhaite diriger des routes internes vers l'unité active.

Étape 2 Configurez les informations d'authentification du principal de service Azure :

failover cloud authentication {**application-id** | **directory-id** | **key**}

Pour modifier les tables de routage Azure lors d'un basculement, vous devez obtenir une *clé d'accès* auprès de l'infrastructure Azure avant de pouvoir accéder aux tables de routage. Vous obtenez la *clé d'accès* en utilisant un ID d'application, un ID de répertoire et une clé secrète pour le principal de service Azure qui contrôle la paire à haute accessibilité.

Étape 3 Configurez l'ID d'application du principal de service Azure :

failover cloud authentication application-id *appl-id*

Exemple :

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e4201
```

Vous avez besoin de cet ID d'application lorsque vous demandez une clé d'accès auprès de l'infrastructure Azure.

Étape 4 Configurez l'ID de répertoire du principal de service Azure :

failover cloud authentication directory-id *dir-id*

Exemple :

```
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
```

Vous avez besoin de cet ID de répertoire lorsque vous demandez une clé d'accès auprès de l'infrastructure Azure.

Étape 5 Configurez l'ID de clé secrète du principal de service Azure :

failover cloud authentication key *secret-key* [**encrypt**]

Exemple :

```
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
```

Vous avez besoin de cette clé secrète lorsque vous demandez une clé d'accès auprès de l'infrastructure Azure. Si le mot clé **encrypt** est présent, la clé secrète est chiffrée dans la commande **running-config**.

Configurer les tableaux de routage Azure

La configuration de la table de routage comprend des renseignements sur les routes définies par l'utilisateur Azure qui doivent être mises à jour lorsque l'ASA virtuel assume le rôle actif. Lors du basculement, vous souhaitez diriger des routes internes vers l'unité active, qui utilise les renseignements de la table de routage configurée pour diriger automatiquement les routes vers elle-même.

Remarque Vous devez configurer tous les renseignements de la table de routage Azure sur les unités actives et de sauvegarde.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.
- Configurez ces paramètres sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire.
- Ayez les renseignements sur votre environnement Azure à disposition, y compris votre ID d'abonnement Azure et vos informations d'authentification Azure pour le principal du service.

Procédure

Étape 1 Configurez une table de routage Azure qui nécessite une mise à jour lors d'un basculement :

failover cloud route-table *table-name* [**subscription-id** *sub-id*]

Exemple :

```
ciscoasa(config)# failover cloud route-table inside-rt
```

(Facultatif) Pour mettre à jour des routes définies par l'utilisateur dans plusieurs abonnement Azure, incluez le paramètre **subscription-id**.

Exemple :

```
ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
```

Le paramètre **subscription-id** au niveau de la commande **route-table** remplace l'ID d'abonnement Azure spécifié au niveau global. Si vous entrez la commande **route-table** sans préciser d'ID d'abonnement Azure, le paramètre global **subscription-id** est utilisé. Consultez Configurer les informations d'authentification pour un principal de service Azure, à la page 344 pour en savoir pl sur l'ID d'abonnement Azure.

Remarque
Lorsque vous saisissez la commande **route-table**, l'ASA virtuel passe en mode **cfg-fover-cloud-rt** .

Étape 2 Configurez un groupe de ressources Azure pour une table de routage :

rg *resource-group*

Exemple :

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
```

Vous avez besoin d'un groupe de ressources pour les demandes de mise à jour de la table de routage dans Azure.

Étape 3 Configurez une route qui nécessite une mise à jour lors d'un basculement :

route name *route-name* **prefix** *address-prefix* **nexthop** *ip-address*

Exemple :

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
```

Le préfixe d'adresse est configuré comme un préfixe d'adresse IP, une barre oblique (« / ») et un masque réseau numérique. Par exemple, *192.120.0.0/16*.

Exemple

Exemple de configuration complète :

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4
```

Activer le basculement actif/de secours

Vous activez le basculement actif/de secours après avoir configuré les paramètres sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.

Activer l'unité principale pour le basculement actif/de secours

Suivez les étapes de cette section pour activer l'unité principale dans une configuration de basculement actif/de secours.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Étape 1 Activez le basculement :

ciscoasa(config)# failover

Étape 2 Enregistrez la configuration système dans la mémoire flash :

ciscoasa(config)# write memory

Exemple

L'exemple suivant montre une configuration complète pour l'unité principale :

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.4

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44
```

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

Prochaine étape

Activez l'unité secondaire.

Activer l'unité secondaire pour le basculement actif/de secours

Suivez les étapes de cette section pour activer l'unité secondaire dans une configuration de basculement actif/de secours.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Étape 1 Activez le basculement :

ciscoasa(config)# **failover**

Étape 2 Enregistrez la configuration système dans la mémoire flash :

ciscoasa(config)# **write memory**

Exemple

L'exemple suivant montre une configuration complète pour l'unité secondaire :

```
ciscoasa(config)# failover cloud unit secondary
ciscoasa(config)# failover cloud peer ip 10.4.3.5

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
```

```
ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

Gérer le basculement dans le nuage public

Cette section décrit comment gérer les unités Failover (basculement) dans le nuage après avoir activé le basculement, y compris comment forcer le basculement d'une unité à une autre.

Forcer le basculement

Pour forcer l'unité en veille à devenir active, exécutez la commande suivante.

Avant de commencer

Utilisez cette commande dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Étape 1 Forcez un basculement lorsque vous avez saisi la commande sur l'unité *en veille* :

failover active

Exemple :

```
ciscoasa# failover active
```

L'unité en veille devient l'unité active.

Étape 2 Forcez un basculement lorsque vous avez saisi la commande sur l'unité *active* :

no failover active

Exemple :

```
ciscoasa# no failover active
```

L'unité active devient l'unité en veille.

Mettre à jour les routes

Si l'état des routes dans Azure est incohérent avec l'ASA virtuel dans le rôle *actif*, vous pouvez forcer les mises à jour de routes sur l'ASA virtuel à l'aide de la commande EXEC suivante :

Avant de commencer

Utilisez cette commande dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Mettez à jour les routes sur l'unité *active* :

failover cloud update routes

Exemple :

```
ciscoasa# failover cloud update routes
Beginning route-table updates
Routes changed
```

Cette commande est uniquement valide sur l'ASA virtuel dans le rôle *actif*. Si l'authentification échoue, la sortie de la commande sera `Route changes failed`.

Valider l'authentification Azure

Pour un déploiement réussi de l'ASA virtuel à haute disponibilité dans Azure, la configuration du principal de service doit être complète et précise. Sans l'autorisation Azure appropriée, les unités ASA virtuel ne pourront pas accéder aux ressources pour gérer le basculement et effectuer des mises à jour de routage. Vous pouvez tester votre configuration de basculement pour détecter les erreurs liées aux éléments suivants de votre principal de service Azure :

- ID de répertoire
- ID d'application
- Clé d'authentification

Avant de commencer

Utilisez cette commande dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Testez les éléments d'authentification Azure dans votre configuration ASA virtuel à haute disponibilité :

test failover cloud authentication

Exemple :

```
ciscoasa(config)# test failover cloud authentication
Checking authentication to cloud provider
Authentication Succeeded
```

Si l'authentification échoue, la sortie de la commande sera `Authentication Failed` (Échec d'authentification).

Si l'ID de répertoire ou l'ID d'application n'est pas configuré correctement, Azure ne reconnaîtra pas la ressource mentionnée dans la demande REST pour obtenir un jeton d'authentification. L'historique des événements pour cette entrée de condition indiquera :

```
Error Connection - Unexpected status in response to access token request: Bad Request
```

Si l'ID de répertoire ou l'ID d'application sont corrects, mais que la clé d'authentification n'est pas configurée correctement, Azure n'accordera pas l'autorisation de générer le jeton d'authentification. L'historique des événements pour cette entrée de condition indiquera :

```
Error Connection - Unexpected status in response to access token request: Unauthorized
```

Superviser le basculement dans le nuage public

Cette section explique comment superviser l'état du basculement.

État de basculement

Pour superviser l'état du basculement, saisissez l'une des commandes suivantes :

- **show failover**

  Affiche des renseignements sur l'état de basculement de l'unité. Les valeurs des éléments de configuration qui n'ont pas été configurés afficheront *non configuré*.

  Les renseignements de mise à jour du routage sont présentés uniquement pour l'unité active.

- **show failover history**

  Affiche l'historique des événements de basculement avec un horodatage, un niveau de gravité, un type d'événement et un texte d'événement.

Messages de basculement

Messages de journal système de basculement

L'ASA émet un certain nombre de messages de journal système liés au basculement au niveau de priorité 2, ce qui indique une condition critique. Pour afficher ces messages, consultez le guide des messages du journal système. Les messages de journal système sont compris entre 1045xx et 1055xx.

Remarque Pendant le basculement, l'ASA s'éteint de manière logique, puis affiche des interfaces, générant des messages de journal système. Il s'agit d'une activité normale.

Voici des exemples de journaux système générés lors d'un basculement :

```
%ASA-3-105509: (Primary) Error sending Hello message to peer unit 10.22.3.5, error: Unknown
 error
%ASA-1-104500: (Primary) Switching to ACTIVE - switch reason: Unable to send message to
Active unit
```

```
%ASA-5-105522: (Primary) Updating route-table wc-rt-inside
%ASA-5-105523: (Primary) Updated route-table wc-rt-inside
%ASA-5-105522: (Primary) Updating route-table wc-rt-outside
%ASA-5-105523: (Primary) Updated route-table wc-rt-outside
%ASA-5-105542: (Primary) Enabling load balancer probe responses
%ASA-5-105503: (Primary) Internal state changed from Backup to Active no peer
%ASA-5-105520: (Primary) Responding to Azure Load Balancer probes
```

Chaque journal système lié à un déploiement dans le nuage public est précédé du rôle de l'unité : (Principal) ou (Secondaire).

Messages de débogage de basculement

Pour afficher les messages de débogage, saisissez la commande **debug fover**. Consultez la référence de commande pour en savoir plus.



Remarque Étant donné que la sortie de débogage se voit attribuer une priorité élevée dans le processus du CPU, elle peut affecter considérablement les performances du système. Par conséquent, les commandes **debug fover** doivent uniquement être utilisées pour résoudre des problèmes spécifiques ou au cours de sessions de dépannage effectuées avec le TAC de Cisco.

Interruptions de basculement SNMP

Pour recevoir des alertes SNMP de journal système pour le basculement, configurez l'agent SNMP pour envoyer des alertes SNMP aux stations de gestion SNMP, définissez un hôte de journal système et compilez la MIB de journal système Cisco dans votre station de gestion SNMP.

Historique de basculement dans le nuage public

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement actif/de sauvegarde sur Microsoft Azure	9.8(200)	Cette fonctionnalité a été introduite.



CHAPITRE 10

Grappe ASA pour le Secure Firewall 3100

La mise en grappe vous permet de regrouper plusieurs ASA en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 429.

- À propos de la mise en grappe d'ASA, à la page 353
- Licences pour la mise en grappe d'ASA, à la page 357
- Exigences et conditions préalables à la mise en grappe ASA, à la page 358
- Lignes directrices de la mise en grappe, à la page 360
- Configurer la mise en grappe ASA, à la page 365
- Gérer les nœuds de la grappe, à la page 398
- Supervision de la grappe ASA, à la page 403
- Exemples de mise en grappe ASA, à la page 415
- Référence pour la mise en grappe, à la page 428
- Historique de la mise en grappe d'ASA pour le Secure Firewall , à la page 444

À propos de la mise en grappe d'ASA

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

Intégration de la grappe dans votre réseau

La grappe se compose de plusieurs pare-feu agissant comme une seule unité. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau de fond de panier isolé à grande vitesse pour la communication intra-grappe, connu sous le nom de *liaison de commande de grappe*.
- Accès de gestion à chaque pare-feu pour la configuration et la surveillance.

Lorsque vous placez la grappe dans votre réseau, les routeurs en amont et en aval doivent être en mesure d'équilibrer la charge des données entrant et sortant de la grappe à l'aide EtherChannels étendus. Les interfaces de plusieurs membres de la grappe sont regroupées dans un seul EtherChannel; l'EtherChannel effectue l'équilibrage de la charge entre les unités.

Membres de la grappe

Les membres de la grappe collaborent pour partager la politique de sécurité et les flux de trafic. Cette section décrit la nature de chaque rôle de membre.

Configuration du démarrage

Sur chaque appareil, vous configurez une configuration de démarrage minimale qui inclut le nom de la grappe, l'interface de la liaison de commande de grappe et les autres paramètres de la grappe. Le premier nœud sur lequel vous activez la mise en grappe devient généralement le nœud de *contrôle*. Lorsque vous activez la mise en grappe sur les nœuds suivants, ils rejoignent la grappe en tant que nœuds de *données*.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité dans la configuration de démarrage. la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds de données. En règle générale, lorsque vous créez une grappe pour la première fois, le premier nœud que vous ajoutez devient le nœud de contrôle simplement parce que c'est le seul nœud de la grappe à ce moment-là.

Vous devez effectuer toute la configuration (à l'exception de la configuration de démarrage) sur le nœud de contrôle uniquement; la configuration est ensuite reproduite sur les nœuds de données. Dans le cas de ressources physiques, telles que les interfaces, la configuration du nœud de contrôle est reflétée sur tous les nœuds de données. Par exemple, si vous configurez Ethernet 1/2 comme interface interne et Ethernet 1/1 comme interface externe, ces interfaces sont également utilisées sur les nœuds de données en tant qu'interfaces interne et externe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

Interfaces de la grappe

Vous pouvez configurer des interfaces de données ou en tant qu'interfaces individuelles . Consultez À propos des interfaces de grappe, à la page 366 pour de plus amples renseignements.



Remarque Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

Liaison de commande de grappe

Chaque unité doit dédier au moins une interface matérielle comme liaison de commande de grappe. Consultez Liaison de commande de grappe, à la page 366 pour de plus amples renseignements.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

Gestion de la grappe ASA

L'un des avantages de l'utilisation de la mise en grappe ASA est la facilité de gestion. Cette section décrit comment gérer la grappe.

Réseau de gestion

Nous vous recommandons de connecter toutes les unités à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Interface de gestion

Pour l'interface de gestion, nous vous conseillons d'utiliser l'une des interfaces de gestion dédiées. Vous pouvez configurer les interfaces de gestion en tant qu'interfaces individuelles (pour les modes routé et transparent) ou en tant qu'interface EtherChannel étendue.

Nous vous conseillons d'utiliser des interfaces individuelles pour la gestion, même si vous utilisez des EtherChannels étendus pour vos interfaces de données. Les interfaces individuelles vous permettent de vous connecter directement à chaque unité si nécessaire, tandis qu'une interface EtherChannel étendue ne permet qu'une connexion à distance à l'unité de contrôle actuelle.

Remarque vous ne pouvez pas activer le routage dynamique pour l'interface de gestion. Vous devez utiliser une route statique.

Pour une interface individuelle, l'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours à l'unité de contrôle actuelle. Pour chaque interface, vous configurez également une plage d'adresses de sorte que chaque unité, y compris l'unité de contrôle actuelle, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de gestion cohérent à une adresse; lorsqu'une unité de contrôle change, l'adresse IP de la grappe principale est déplacée vers la nouvelle unité de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente. L'adresse IP locale est utilisée pour le routage et est également utile pour la résolution de problèmes.

Par exemple, vous pouvez gérer la grappe en vous connectant à l'adresse IP de la grappe principale, qui est toujours associée à l'unité de contrôle actuelle. Pour gérer un membre, vous pouvez vous connecter à l'adresse IP locale.

Remarque Le trafic vers la boîte doit être acheminé vers l'adresse IP de gestion du nœud; le trafic vers la boîte n'est pas transféré sur la liaison de commande de grappe vers un autre nœud.

Pour le trafic de gestion sortant tel que TFTP ou syslog, chaque unité, y compris l'unité de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Pour une interface EtherChannel étendue, vous ne pouvez configurer qu'une seule adresse IP, et cette adresse IP est toujours associée à l'unité de contrôle. Vous ne pouvez pas vous connecter directement à une unité de données à l'aide de l'interface EtherChannel; nous vous conseillons de configurer l'interface de gestion en tant qu'interface individuelle afin que vous puissiez vous connecter à chaque unité. Notez que vous pouvez utiliser un EtherChannel local au périphérique pour la gestion.

Gestion de l'unité de contrôle vs Gestion de l'unité de données

Toutes la gestion et la surveillance peuvent avoir lieu sur le nœud de contrôle. À partir du nœud de contrôle, vous pouvez vérifier les statistiques d'exécution, l'utilisation des ressources ou d'autres informations de surveillance sur tous les nœuds. Vous pouvez également transmettre une commande à tous les nœuds de la grappe et reproduire les messages de console des nœuds de données vers le nœud de contrôle.

Vous pouvez surveiller directement les nœuds de données si vous le souhaitez. Bien que cela soit également disponible à partir du nœud de contrôle, vous pouvez effectuer la gestion de fichiers sur les nœuds de données (y compris la sauvegarde de la configuration et la mise à jour des images). Les fonctions suivantes ne sont pas disponibles à partir du nœud de commande :

- Surveillance des statistiques propres à la grappe par nœud.
- Surveillance des journaux système par nœud (sauf pour les journaux système envoyés à la console lorsque la duplication de la console est activée).
- SNMP
- NetFlow

duplication de clé de chiffrement

Lorsque vous créez une clé de chiffrement sur le nœud de contrôle, la clé est répliquée sur tous les nœuds de données. Si vous avez une session SSH sur l'adresse IP de la grappe principale, vous serez déconnecté en cas de défaillance du nœud de contrôle. Le nouveau nœud de contrôle utilise la même clé pour les connexions SSH, de sorte que vous n'avez pas besoin de mettre à jour la clé d'hôte SSH mise en cache lorsque vous vous reconnectez au nouveau nœud de contrôle.

Incompatibilité d'adresse IP du certificat de connexion ASDM

Par défaut, un certificat autosigné est utilisé pour la connexion ASDM en fonction de l'adresse IP locale. Si vous vous connectez à l'adresse IP de la grappe principale à l'aide d'ASDM, un message d'avertissement concernant une adresse IP non concordante peut s'afficher, car le certificat utilise l'adresse IP locale, et non l'adresse IP de la grappe principale. Vous pouvez ignorer le message et établir la connexion ASDM. Cependant, pour éviter ce type d'avertissement, vous pouvez inscrire un certificat qui contient l'adresse IP de la grappe principale et toutes les adresses IP locales de l'ensemble d'adresses IP. Vous pouvez ensuite utiliser ce certificat pour chaque membre de la grappe. Consultez https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html pour de plus amples renseignements.

Mise en grappe inter-sites

Pour les installations inter-sites, vous pouvez profiter de la mise en grappe d'ASA tant que vous suivez les lignes directrices recommandées.

Vous pouvez configurer chaque châssis de grappe pour qu'il appartienne à un ID de site distinct.

Les ID de site fonctionnent avec des adresses MAC et des adresses IPspécifiques au site . Les paquets qui sortent de la grappe utilisent une adresse MAC et une adresse IPpropres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IPglobales. Cette fonctionnalité empêche les commutateurs d'apprendre la même adresse MAC globale à partir des deux sites sur deux ports différents, ce qui entraîne une oscillation MAC; au lieu de cela, ils connaissent uniquement l'adresse MAC du site. Les adresses MAC et les adresses IP spécifiques au site sont prises en charge pour le mode routé qui utilise uniquement les EtherChannels étendus.

Les ID de site sont également utilisés pour permettre la mobilité de flux à l'aide de l'inspection LISP, la localisation du directeur pour améliorer les performances et réduire la latence aller-retour pour la mise en grappe inter-sites pour les centres de données, et la redondance des sites pour les connexions où un propriétaire de secours d'un flux se trouve toujours sur un autre site que celui du propriétaire.

Consultez les sections suivantes pour en savoir plus sur la mise en grappe inter-sites :

- Dimensionnement de l'interconnexion du centre de données : Exigences et conditions préalables à la mise en grappe ASA, à la page 358
- Lignes directrices inter-sites : Lignes directrices de la mise en grappe, à la page 360
- Configurer la mobilité des flux de grappes : Configurer la mobilité des flux de grappes, à la page 393
- Activer la localisation du directeur : Activer la localisation du directeur, à la page 391
- Activer la redondance de site : Activer la localisation du directeur, à la page 391
- Exemples inter-sites : Exemples de mise en grappe inter-sites, à la page 425

Licences pour la mise en grappe d'ASA

Smart Software Manager standard et sur site

Chaque unité requiert la licence Essentials (activée par défaut) et la même licence de chiffrement. Nous vous conseillons d'accorder une licence à chaque unité avec le serveur de licences *avant* d'activer la mise en grappe pour éviter les problèmes de non-concordance de licences et, lors de l'utilisation de la licence de cryptage renforcé, des problèmes de chiffrement de la liaison de commande de grappe.

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Il n'y a pas de coût supplémentaire pour la licence de contexte sur les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, la licence Essentials est toujours activée par défaut sur toutes les unités. Vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : chaque unité demande une licence Essentials au serveur.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 2 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence

Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :

- Vous avez 6 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 6 unités, ces licences ajoutent jusqu'à 12 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 32 contextes. Comme la limite de plateformes pour un châssis est de 100, la licence combinée autorise un maximum de 100 contextes; les 32 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 32 contextes sur l'unité de contrôle; chaque unité de données aura également 32 contextes par la réplication de la configuration.
- Vous avez 3 appareils Secure Firewall 3100 dans la grappe. La licence Essentials comprend 2 contextes; pour 3 unités, ces licences ajoutent jusqu'à 6 contextes. Vous configurez une licence de 100 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 106 contextes. Comme la limite de plateformes pour une unité est de 100, la licence combinée autorise un maximum de 100 contextes; les 106 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 100 contextes sur l'unité de contrôle; chaque unité de données aura également 100 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 94 contextes.

- Cryptage renforcé (3DES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Seule l'unité de contrôle demande cette licence et toutes les unités peuvent l'utiliser en raison de l'agrégation des licences.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement des droits d'utilisation toutes les 35 secondes jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Exigences et conditions préalables à la mise en grappe ASA

Exigences du modèle

- Secure Firewall 3100 : maximum de ,8 unités

Configuration matérielle et logicielle requise pour l'ASA

Pour toutes les unités d'une grappe :

- Doivent être du même modèle et disposer de la même mémoire DRAM. Vous n'avez pas besoin d'avoir la même quantité de mémoire flash.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Doivent être dans le même mode de contexte de sécurité, unique ou multiple.
- (Mode de contexte unique) Doivent utiliser le même mode de pare-feu (routé ou transparent).
- Les nouveaux membres de la grappe doivent utiliser le même paramètre de chiffrement SSL (la commande **ssl encryption**) que l'unité de contrôle pour la communication de la liaison de commande de grappe initiale avant la réplication de la configuration.

Exigences du commutateur

- Assurez-vous d'achever la configuration du commutateur avant de configurer la mise en grappe sur les ASA.
- Pour obtenir la liste des commutateurs pris en charge, consultez Compatibilité Cisco ASA.

Exigences ASA

- Fournissez à chaque unité une adresse IP unique avant de les joindre au réseau de gestion.
  - Consultez le chapitre de démarrage pour en savoir plus sur la connexion à l'ASA et la définition de l'adresse IP de gestion.
  - À l'exception de l'adresse IP utilisée par l'unité de contrôle (généralement la première unité que vous ajoutez à la grappe), ces adresses IP de gestion sont uniquement destinées à un usage temporaire.
  - Après qu'une unité de données ait rejoint la grappe, la configuration de l'interface de gestion est remplacée par celle répliquée à partir de l'unité de contrôle.

dimensionnement de l'interconnexion du centre de données pour la mise en grappe inter-sites

Vous devez réserver la bande passante sur l'interconnexion des centres de données (DCI) pour un trafic de liaison de commande de grappe équivalent au calcul suivant :

$$\frac{\text{Nombre de membres de grappe par site}}{2} \times \text{liaison de commande de grappe par membre}$$

Si le nombre de membres diffère sur chaque site, utilisez le plus grand nombre pour votre calcul. La bande passante minimale pour l'interface DCI ne doit pas être inférieure à la taille de la liaison de commande de grappe pour un membre.

Par exemple :

- Pour 4 membres sur 2 sites :
  - 4 membres de la grappe au total

- 2 membres sur chaque site
- Liaison de commande de grappe de 5 Gbit/s par membre

Bande passante DCI réservée = 5 Gbit/s (2/2 x 5 Gbit/s).

- Pour 6 membres sur 3 sites, la taille augmente :
  - Six membres de la grappe au total
  - 3 membres sur le site 1, 2 membres sur le site 2 et 1 membre sur le site 3
  - Liaison de commande de grappe de 10 Gbit/s par membre

  Bande passante DCI réservée = 15 Gbit/s (3/2 x 10 Gbit/s).
- Pour 2 membres sur 2 sites :
  - 2 membres de la grappe au total
  - Un membre sur chaque site
  - Liaison de commande de grappe de 10 Gbit/s par membre

  Bande passante DCI réservée = 10 Gbit/s (1/2 x 10 Gbit/s = 5 Gbit/s, mais la bande passante minimale ne doit pas être inférieure à la taille de la liaison de commande de grappe (10 Gbit/s)).

Autres exigences

Nous vous conseillons d'utiliser un serveur de terminaux pour accéder à tous les ports de console des unités membres de la grappe. Pour la configuration initiale et la gestion continue (par exemple, lorsqu'une unité tombe en panne), un serveur de terminaux est utile pour la gestion à distance.

Lignes directrices de la mise en grappe

Mode contextuel

Le mode doit correspondre sur chaque unité membre.

Mode pare-feu

Pour le mode unique, le mode de pare-feu doit correspondre sur toutes les unités.

Basculement

Le basculement n'est pas pris en charge avec la mise en grappe.

IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

Commutateurs

- Assurez-vous que les commutateurs connectés correspondent aux unités de transfert maximales MTU des interfaces de données et de l'interface de liaison de commande de grappe. Vous devez configurer la MTU de l'interface de la liaison de commande de grappe pour qu'elle soit au moins 100 octets supérieure à la MTU de l'interface de données. Assurez-vous donc de configurer le commutateur de connexion de la liaison de commande de grappe correctement. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe. De plus, nous ne conseillons pas de définir la MTU de la liaison de commande de grappe entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système.
- Pour les systèmes Cisco IOS XR, si vous souhaitez définir une MTU autre que celle par défaut, définissez la MTU de l'interface IOS XR sur 14 octets au-dessus de la MTU du périphérique de la grappe. Sinon, les tentatives d'homologation de contiguïté OSPF peuvent échouer, sauf si l'option **mtu-ignore** est utilisée. Notez que la MTU du périphérique de grappe doit correspondre à la MTU *IPv4* d'IOS XR. Cet ajustement n'est pas nécessaire pour les commutateurs Cisco Catalyst et Cisco Nexus.
- Sur le ou les commutateurs pour les interfaces de liaison de commande de grappe, vous pouvez éventuellement activer Spanning Tree PortFast sur les ports de commutateur connectés à l'unité de la grappe pour accélérer le processus de jonction des nouvelles unités.
- Sur le commutateur, nous vous conseillons d'utiliser l'un des algorithmes d'équilibrage de charges EtherChannel suivants : **source-dest-ip** or **src-dst-mixed-ip-port** (reportez-vous à la commande **port-channel load-balance** de Cisco Nexus OS et Cisco IOS-XE). N'utilisez pas de mot clé **vlan** dans l'algorithme d'équilibrage de charge, car cela pourrait entraîner une répartition inégale du trafic vers les périphériques d'une grappe. *Ne modifiez pas* l'algorithme d'équilibrage de charge par défaut sur le périphérique de la grappe.
- Si vous modifiez l'algorithme d'équilibrage de charge de l'EtherChannel sur le commutateur, l'interface EtherChannel du commutateur arrête temporairement de transférer le trafic et le protocole Spanning Tree redémarre. Il faudra attendre un certain temps avant que le trafic ne redevienne fluide.
- Les commutateurs sur le chemin de la liaison de commande de grappe ne doivent pas vérifier la somme de contrôle L4. Le trafic redirigé sur la liaison de commande de grappe n'a pas une somme de contrôle L4 correcte. Les commutateurs qui vérifient la somme de contrôle L4 pourraient entraîner l'abandon du trafic.
- Le temps d'arrêt du groupage du canal de port ne doit pas dépasser l'intervalle Keepalive configuré.
- Sur les EtherChannels de 2e génération, l'algorithme de distribution de hachage par défaut est adaptatif. Pour éviter le trafic symétrique dans une conception VSS, modifiez l'algorithme de hachage sur le canal de port connecté au périphérique de la grappe à fixe :

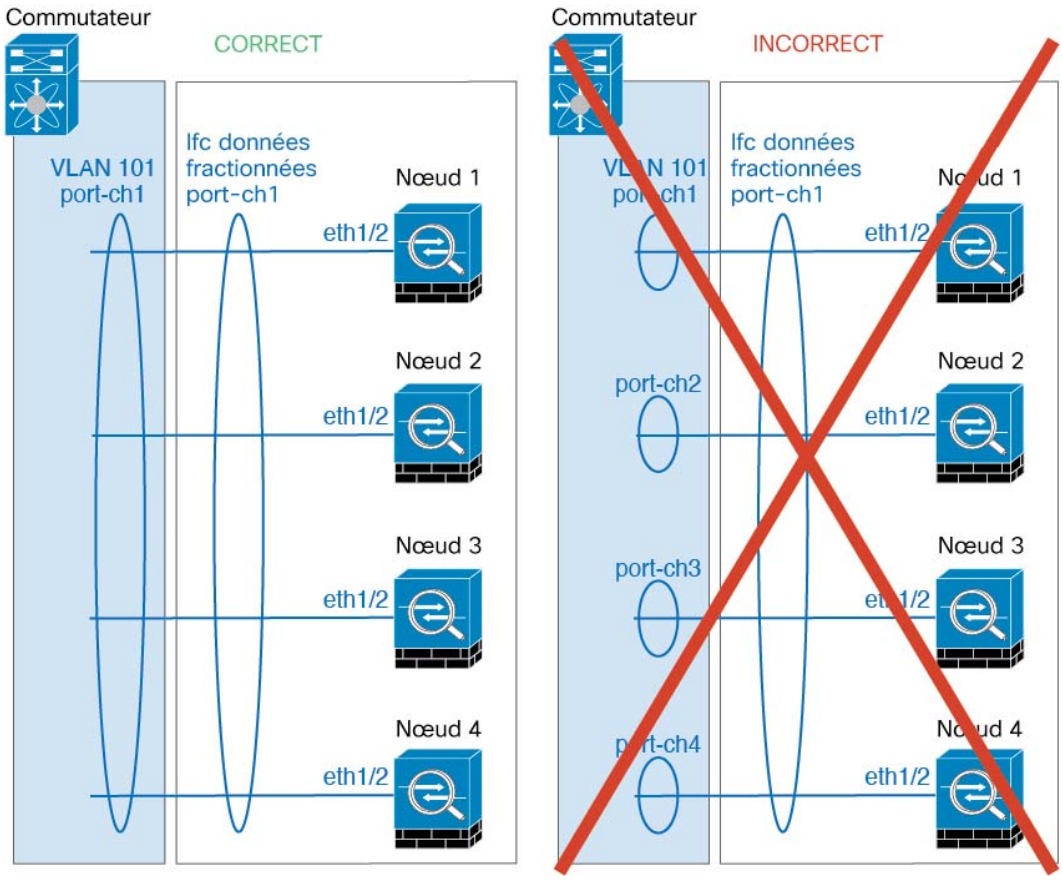
  router(config)# **port-channel** *id* **hash-distribution fixed**

  Ne modifiez pas l'algorithme globalement; vous pouvez profiter de l'algorithme adaptatif pour la liaison homologue VSS.

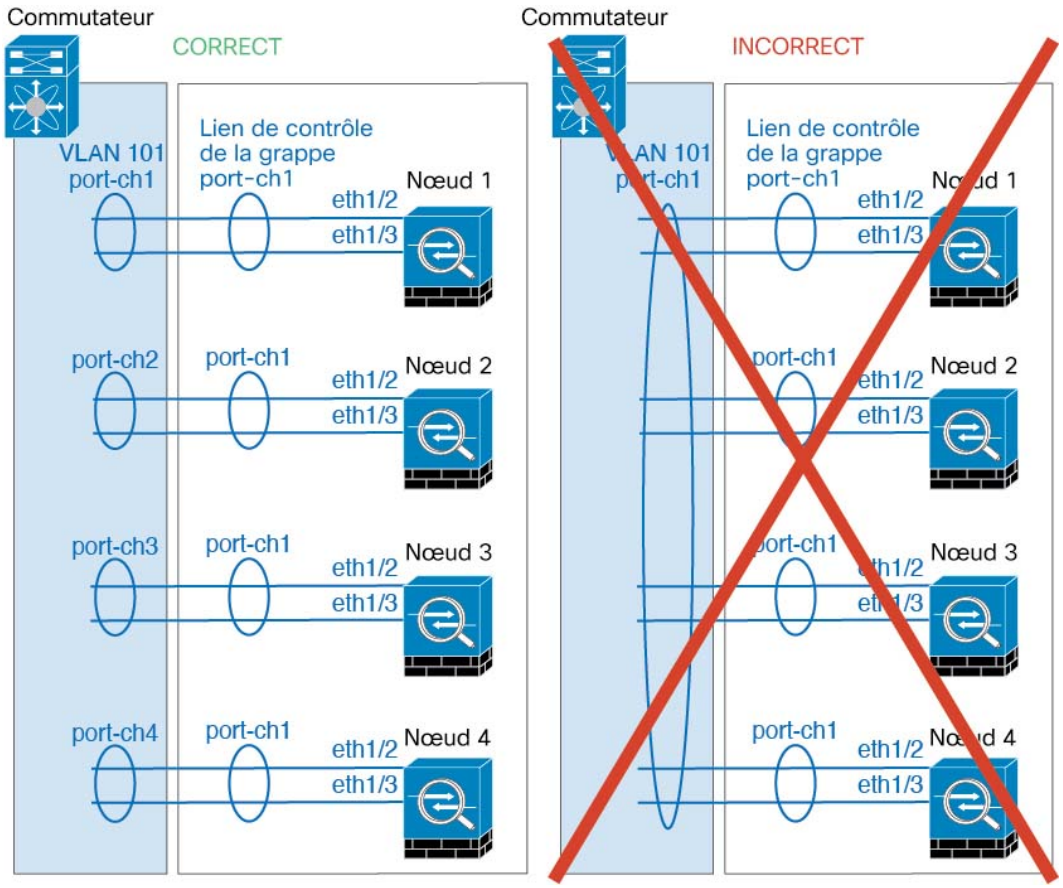
- Vous devez désactiver la fonctionnalité de convergence progressive LACP sur toutes les interfaces EtherChannel face à la grappe pour les commutateurs Cisco Nexus.

EtherChannels

- Dans les versions du logiciel Cisco IOS Catalyst 3750-X antérieures à la15.1(1)S2, l'unité de grappe ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel de l'unité de grappe est connecté de manière croisée et si le commutateur de l'unité de contrôle est hors tension, l'EtherChannel connecté au commutateur restant ne s'activera pas. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.
- Configuration des EtherChannels étendus vs. locaux au périphérique : veillez à configurer le commutateur de manière appropriée pour les EtherChannels étendus par rapport aux EtherChannels locaux au périphérique.
  - EtherChannels étendus : pour les EtherChannels *étendus* des unités de grappe, qui s'étendent sur tous les membres de la grappe, les interfaces sont combinées en un seul EtherChannel sur le commutateur. Vérifiez que chaque interface se trouve dans le même groupe de canaux sur le commutateur.



  - EtherChannels locaux au périphérique : pour les EtherChannels *locaux au périphérique* de grappe, y compris tous les EtherChannels configurés pour la liaison de commande de la grappe, veillez à configurer des EtherChannels isolés sur le commutateur; ne combinez pas plusieurs EtherChannels d'unités de grappe en un seul EtherChannel sur le commutateur.



Lignes directrices inter-sites

Consultez les consignes suivantes concernant la mise en grappe inter-sites :

- La latence de la liaison de commande de grappe doit être inférieure à 20 ms temps aller-retour (RTT).
- La liaison de commande de grappe doit être fiable, sans paquets dans le désordre ou abandonnés; par exemple, vous devez utiliser un lien dédié.
- Ne configurez pas le rééquilibrage de connexion; il ne faut pas que les connexions soient rééquilibrées entre les membres de la grappe sur un site différent.
- Le ASA ne chiffre pas le trafic de données transféré sur la liaison de commande de grappe, car il s'agit d'un lien dédié, même lorsqu'il est utilisé sur une interconnexion de centre de données (DCI). Si vous utilisez la virtualisation du transport par superposition (OTV), ou étendez la liaison de commande de grappe en dehors du domaine administratif local, vous pouvez configurer le chiffrement sur vos routeurs de frontière, comme 802.1AE MacSec sur OTV.
- La mise en œuvre de la grappe ne fait pas de différence entre les membres de plusieurs sites pour les connexions entrantes; par conséquent, les rôles de connexion pour une connexion donnée peuvent s'étendre sur plusieurs sites. Il s'agit du comportement attendu. Toutefois, si vous activez la localisation de directeur, le rôle de directeur local est toujours choisi sur le même site que le propriétaire de la connexion (selon l'ID du site). En outre, le directeur local choisit un nouveau propriétaire sur le même site si le propriétaire d'origine tombe en panne (Remarque : si le trafic est dissymétrique entre les sites et qu'il y a un trafic

continu en provenance du site distant après la défaillance du propriétaire d'origine, alors un nœud du site distant site peut devenir le nouveau propriétaire s'il reçoit un paquet de données pendant la fenêtre de réhébergement.).

- Pour la localisation du directeur, les types de trafic suivants ne prennent pas en charge la localisation : le trafic NAT ou PAT; trafic inspecté par SCTP; requête du propriétaire de la fragmentation.
- Dans un déploiement Nord-Sud avec des flux UDP persistants, des boucles de routage peuvent se produire si les nœuds du site propriétaire initial du flux tombent en panne, puis reviennent en ligne, ce qui entraîne une redirection du flux vers le site d'origine. Si le nouveau propriétaire, sur l'autre site, ne dispose pas d'une route vers la destination, il redirigera le flux vers Internet, créant ainsi une boucle. Dans ce cas, utilisez la commande **clear conn** sur le nouveau propriétaire pour forcer la réinitialisation du flux.
- Pour le mode transparent, si la grappe est placée entre une paire de routeurs internes et externes (AKA insertion nord-sud), vous devez vous assurer que les deux routeurs internes partagent une adresse MAC et que les deux routeurs externes partagent une adresse MAC. Lorsqu'un membre de la grappe sur le site 1 transfère une connexion à un membre du site 2, l'adresse MAC de destination est conservée. Le paquet n'atteindra le routeur du site 2 que si l'adresse MAC est la même que celle du routeur du site 1.
- Pour le mode transparent, si la grappe est placée entre les réseaux de données et le routeur de passerelle de chaque site pour le pare-feu entre les réseaux internes (AKA insertion est-ouest), chaque routeur de passerelle doit utiliser un protocole FHRP (First Hop Redundancy Protocol) comme HSRP pour fournir des destinations d'adresses IP et MAC virtuelles identiques sur chaque site. Les VLAN de données sont étendus à l'ensemble des sites à l'aide de la virtualisation du transport par superposition (OTV), ou d'un outil similaire. Vous devez créer des filtres pour empêcher le trafic destiné au routeur de la passerelle local d'être envoyé à l'autre site sur DCI. Si le routeur de la passerelle devient inaccessible sur un site, vous devez supprimer les filtres pour que le trafic puisse atteindre la passerelle de l'autre site.
- Pour le mode transparent, si la grappe est connectée à un routeur HSRP, vous devez ajouter l'adresse MAC HSRP du routeur en tant qu'entrée de tableau d'adresses MAC statiques sur ASA (voir Ajouter une adresse MAC statique pour les groupes de ponts, à la page 929). Lorsque des routeurs adjacents utilisent HSRP, le trafic destiné à l'adresse IP HSRP sera envoyé à l'adresse MAC HSRP, mais le trafic retour proviendra de l'adresse MAC de l'interface d'un routeur particulier dans la paire HSRP. Par conséquent, le tableau d'adresses MAC ASA n'est généralement mis à jour que lorsque l'entrée du tableau ARP ASA pour l'adresse IP HSRP expire et que le ASA envoie une demande ARP et reçoit une réponse. Étant donné que les entrées du tableau ARP de ASAexpirent après 14 400 secondes par défaut, mais que l'entrée du tableau d'adresses MAC expire après 300 secondes par défaut, une entrée d'adresse MAC statique est requise pour éviter les pertes de trafic liées à l'expiration du tableau.
- Pour le mode routé à l'aide de l'EtherChannel étendu, configurez les adresses MAC propres au site. Étendre les VLAN de données à tous les sites à l'aide d'OTV ou d'un outil similaire. Vous devez créer des filtres pour empêcher le trafic destiné à l'adresse MAC globale d'être envoyé à l'autre site par DCI. Si la grappe devient inaccessible sur un site, vous devez supprimer les filtres pour que le trafic puisse atteindre les nœuds de la grappe de l'autre site. Le routage dynamique n'est pas pris en charge lorsqu'une grappe inter-sites sert de routeur de premier saut pour un segment étendu.

Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le pare-feu ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise, ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées.

Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.

- Lors de l'ajout d'une unité à une grappe existante ou lors du rechargement d'une unité, il se produira une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Si vous utilisez un serveur Windows 2003 connecté à un EtherChannel étendu, lorsque le port du serveur de journal système est en panne et que le serveur ne gère pas les messages d'erreur ICMP, un grand nombre de messages ICMP sont renvoyés à la grappe. Ces messages peuvent faire en sorte que certaines unités de la grappe connaissent un niveau élevé de CPU, ce qui peut affecter les performances. Nous vous recommandons de limiter les messages d'erreur ICMP.
- Il faut du temps pour répliquer les modifications sur toutes les unités d'une grappe. Si vous apportez une modification importante, par exemple, ajouter une règle de contrôle d'accès qui utilise des groupes d'objets (qui, lorsqu'ils sont déployés, sont divisés en plusieurs règles), le temps nécessaire pour effectuer la modification peut dépasser le délai d'expiration des unités de la grappe avec un message de réussite. Si cela se produit, vous pourriez voir le message « Échec de la réplication de la commande ». Vous pouvez ignorer le message.

Valeurs par défaut pour la mise en grappe

- Lorsque vous utilisez des EtherChannels étendus, l'ID système cLACP est généré automatiquement et la priorité du système est 1 par défaut.
- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Le rééquilibrage de la connexion est désactivé par défaut. Si vous activez le rééquilibrage de la connexion, l'intervalle par défaut entre les échanges d'informations de chargement est de 5 secondes.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe ASA

Pour configurer la mise en grappe, effectuez les tâches suivantes.

Remarque Pour activer ou désactiver la mise en grappe, vous devez utiliser une connexion de console (pour l'interface de ligne de commande) ou une connexion ASDM.

Câbler les unités et configurer les interfaces

Avant de configurer la mise en grappe, câblez le réseau de liaisons de commande de grappe, le réseau de gestion et les réseaux de données. Configurez ensuite vos interfaces.

À propos des interfaces de grappe

Vous pouvez configurer des interfaces de données canaux EtherChannels étendus.

Chaque unité doit également dédier au moins une interface matérielle comme liaison de commande de grappe.

Liaison de commande de grappe

Chaque unité doit dédier au moins une interface matérielle comme liaison de commande de grappe. Nous vous recommandons d'utiliser un EtherChannel pour le lien de commande de grappe, si disponible.

Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Interfaces et réseau de la liaison de commande de grappe

Vous pouvez utiliser n'importe quelle interface de données pour la liaison de commande de grappe, avec les exceptions suivantes :

- Vous ne pouvez pas utiliser une sous-interface VLAN comme liaison de commande de grappe.
- Vous ne pouvez pas utiliser une interface de gestion Management *x*/*x* comme liaison de commande de grappe, seule ou en tant qu'EtherChannel.

Vous pouvez utiliser un EtherChannel.

Chaque liaison de commande de grappe possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe ASA.

Pour une grappe de deux membres, ne connectez pas directement la liaison de commande de grappe d'un nœud ASA à l'autre ASA. Si vous connectez directement les interfaces, lorsqu'une unité tombe en panne, la liaison de commande de grappe tombe en panne, et donc l'unité intègre restante. Si vous connectez la liaison de commande de grappe par l'intermédiaire d'un commutateur, cette dernière reste active pour l'unité intègre.

Dimensionner la liaison de commande de grappe

Si possible, vous devez dimensionner la liaison de commande de grappe en fonction du débit attendu de chaque châssis afin que la liaison de commande de grappe puisse gérer les scénarios les plus défavorables.

Le trafic de liaison de commande de grappe est principalement composé de mises à jour d'état et de paquets transférés. Le volume de trafic varie à un moment donné sur la liaison de commande de grappe. La quantité de trafic transféré dépend de l'efficacité de l'équilibrage de la charge et de l'importance du trafic pour les fonctionnalités centralisées. Par exemple :

- La NAT entraîne un mauvais équilibrage de la charge des connexions et la nécessité de rééquilibrer tout le trafic de retour vers les bonnes unités.
- L'AAA pour l'accès réseau est une fonctionnalité centralisée, de sorte que tout le trafic est acheminé à l'unité de contrôle.
- Lorsque les membres changent, la grappe doit rééquilibrer un grand nombre de connexions, utilisant ainsi temporairement une grande quantité de bande passante de la liaison de commande de grappe.

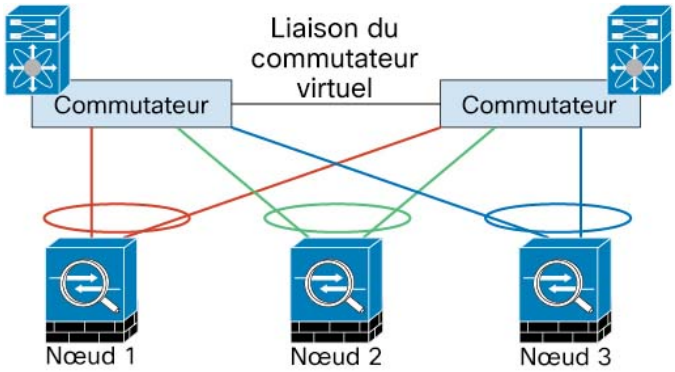
Une liaison de commande de grappe à bande passante plus élevée aide la grappe à converger plus rapidement lorsque les membres changent et empêche les goulots d'étranglement.

Remarque Si votre grappe génère un trafic asymétrique (rééquilibreur) important, vous devez augmenter la taille du lien de commande de grappe.

Redondance de la liaison de commande de la grappe

Nous vous recommandons d'utiliser un EtherChannel pour la liaison de commande de la grappe, afin de pouvoir transférer le trafic sur plusieurs liaisons de l'EtherChannel tout en assurant la redondance.

Le diagramme suivant montre comment utiliser un EtherChannel comme liaison de commande de la grappe dans un système de commutation virtuelle (VSS), un canal de port virtuel (vPC), un StackWise ou un environnement StackWise Virtual. Tous les liens de l'EtherChannel sont actifs. Lorsque le commutateur fait partie d'un système redondant, vous pouvez connecter des interfaces de pare-feu dans le même EtherChannel pour séparer les commutateurs du système redondant. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur. Notez qu'il s'agit d'un EtherChannel local au périphérique et non d'un EtherChannel étendu.



Fiabilité de la liaison de commande de grappe

Pour assurer la fonctionnalité de la liaison de commande de grappe, vérifiez que le temps aller-retour (RTT) entre les unités est inférieur à 20 ms. Cette latence maximale améliore la compatibilité avec les membres de la grappe installés à différents sites géographiques. Pour vérifier votre latence, envoyez un message Ping sur la liaison de commande de grappe entre les unités.

La liaison de commande de grappe doit être fiable, sans paquets en désordre ou abandonnés; par exemple, pour un déploiement intersite, vous devez utiliser un lien dédié.

Échec de la liaison de commande de grappe

Si le protocole de liaison de commande de grappe tombe en panne pour une unité, la mise en grappe est désactivée; les interfaces de données sont fermées. Après avoir corrigé la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.

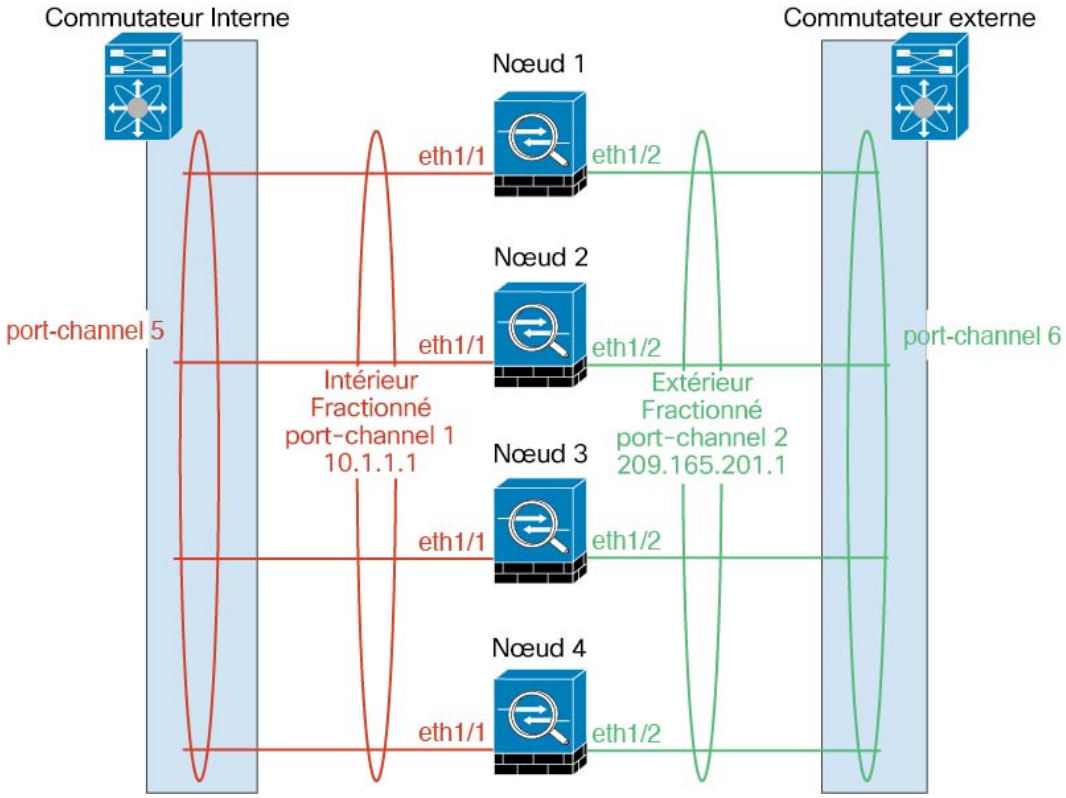
Remarque Lorsque l'ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que l'unité a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que l'unité est toujours inactive dans la grappe, l'interface de gestion n'est pas accessible (car elle utilise alors l'adresse IP principale, qui est la même que l'unité de contrôle). Vous devez utiliser le port de console pour toute autre configuration.

EtherChannels étendus

Vous pouvez regrouper une ou plusieurs interfaces par châssis dans un EtherChannel qui s'étend sur tous les châssis de la grappe. L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal.

Un EtherChannel étendu peut être configuré dans les modes de pare-feu avec routage et transparent. En mode routé, l'EtherChannel est configuré comme une interface routée avec une seule adresse IP. En mode transparent, l'adresse IP est attribuée aux BVI, et non à l'interface du membre du groupe de ponts.

L'EtherChannel assure intrinsèquement l'équilibrage de la charge dans le cadre du fonctionnement de base.



Lignes directrices pour le débit maximal

Pour atteindre un débit maximal, nous vous recommandons ce qui suit :

- Utilisez un algorithme de hachage pour l'équilibrage de la charge qui est « symétrique », ce qui signifie que les paquets des deux directions auront le même hachage et seront envoyés au même ASA dans l'EtherChannel étendu. Nous vous recommandons d'utiliser l'adresse IP source et de destination (par défaut) ou les ports source et destination comme algorithme de hachage.
- Utilisez le même type de cartes de ligne lors de la connexion des ASAau commutateur afin que les algorithmes de hachage appliqués à tous les paquets soient les mêmes.

Équilibrage de la charge

Le lien EtherChannel est sélectionné à l'aide d'un algorithme de hachage propriétaire, en fonction des adresses IP source ou de destination et des numéros de ports TCP et UDP.

Remarque Sur le commutateur, nous vous recommandons d'utiliser l'un des algorithmes suivants : **source-dest-ip** ou **source-dest-ip-port** (consultez la commande **d'équilibrage de la charge du canal de port** du système d'exploitation Cisco Nexus ou Cisco IOS). N'utilisez pas le mot clé **vlan** dans l'algorithme d'équilibrage de charges, car cela pourrait entraîner une répartition inégale du trafic vers les nœuds d'une grappe.

Le nombre de liaisons dans l'EtherChannel affecte l'équilibrage de la charge.

L'équilibrage de charge symétrique n'est pas toujours possible. Si vous configurez la NAT, les paquets de transfert et de retour auront des adresses IP et/ou des ports différents. Le trafic de retour sera envoyé vers une autre unité en fonction du hachage, et la grappe devra rediriger la majeure partie du trafic de retour vers la bonne unité.

Redondance EtherChannel

L'EtherChannel a une redondance intégrée. Il surveille l'état du protocole de ligne de toutes les liaisons. Si une liaison échoue, le trafic est rééquilibré entre les liaisons restantes. Si tous les liens de l'EtherChannel échouent sur une unité particulière, mais que d'autres unités sont toujours actives, cette unité est supprimée de la grappe.

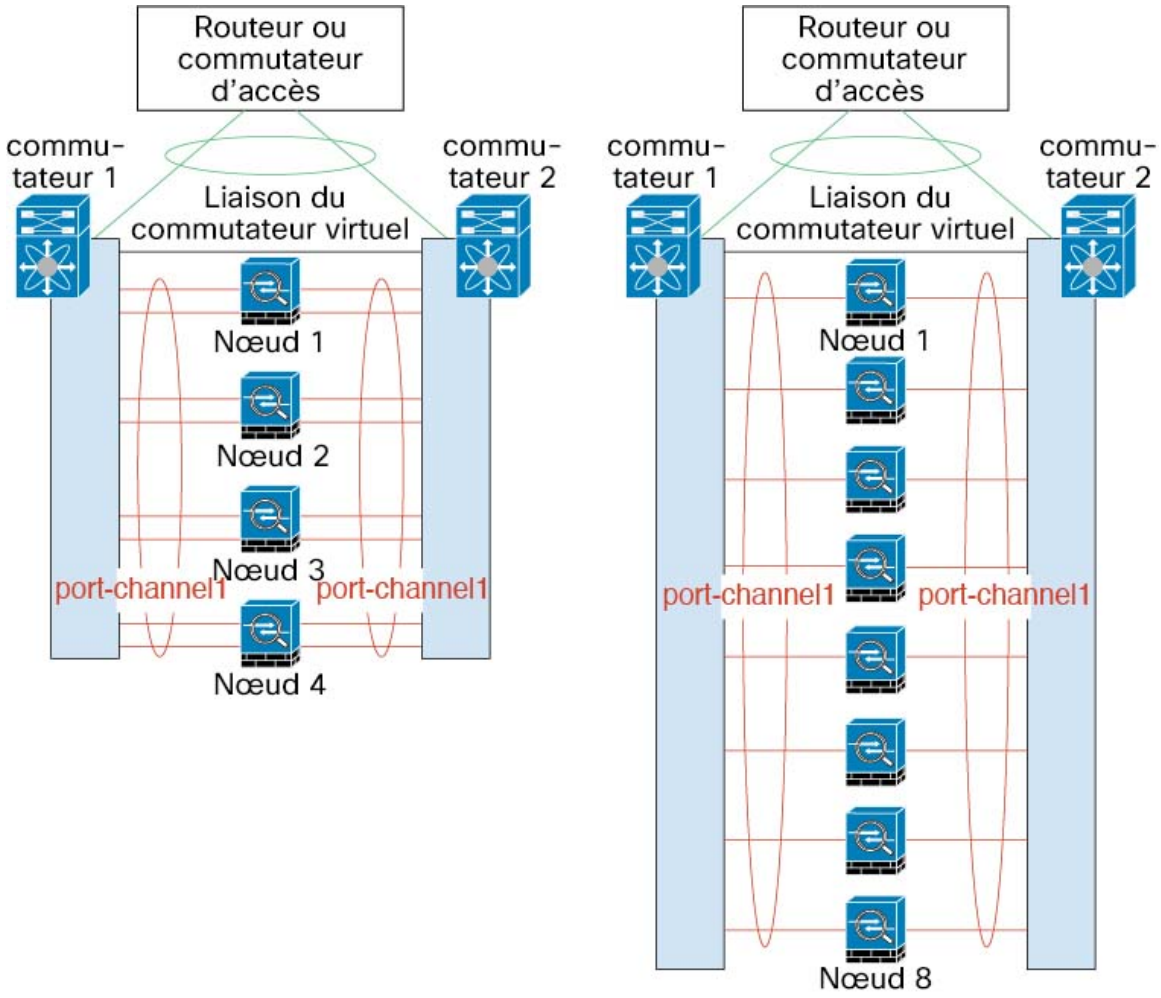
Connexion à un système de commutateurs redondants

Vous pouvez inclure plusieurs interfaces pour chaque ASA dans l'EtherChannel étendu. Plusieurs interfaces par ASA sont particulièrement utiles pour la connexion aux deux commutateurs dans un système VSS, vPC, StackWise ou StackWise Virtual.

Selon vos commutateurs, vous pouvez configurer jusqu'à 32 liens actifs dans l'EtherChannel étendu. Cette fonctionnalité nécessite que les deux commutateurs du vPC prennent en charge les canaux EtherChannels avec 16 liens actifs chacun (par exemple, le module Cisco Nexus 7000 avec le module Ethernet de 10 Gigabit de la gamme F2).

Pour les commutateurs qui prennent en charge 8 liens actifs dans l'EtherChannel, vous pouvez configurer jusqu'à 16 liens actifs dans l'EtherChannel étendu lors de la connexion à deux commutateurs dans un système redondant.

La figure suivante montre un EtherChannel de 16 liens actifs dans une grappe de 4 nœuds et une grappe de 8 nœuds.



Câbler les unités de grappe et configurer les équipements en amont et en aval

Avant de configurer la mise en grappe, câblez le réseau de liaisons de commande de grappe, le réseau de gestion et les réseaux de données.

Procédure

Étape 1 Câblez le réseau de liaisons de commande de grappe, le réseau de gestion et les réseaux de données.

Remarque
Au minimum, un réseau de liaison de commande de grappe actif est requis avant de configurer les nœuds pour qu'ils se joignent à la grappe.

Étape 2 Vous devez également configurer les équipements en amont et en aval. Par exemple, si vous utilisez des EtherChannels, vous devez configurer les équipements en amont et en aval pour les EtherChannels.

Configurer le mode d'interface de grappe de chaque unité

Avant d'activer la mise en grappe, vous devez convertir le pare-feu pour utiliser les EtherChannels étendus. Étant donné que la mise en grappe limite les types d'interfaces que vous pouvez utiliser, ce processus vous permet de vérifier votre configuration existante pour détecter les interfaces incompatibles, puis vous empêche de configurer des interfaces non prises en charge.

Avant de commencer

- Vous devez définir le mode séparément sur chaque ASA que vous souhaitez ajouter à la grappe.
- Vous pouvez toujours configurer l'interface de gestion uniquement en tant qu'interface individuelle (conseillé). L'interface de gestion peut être une interface individuelle même en mode de pare-feu transparent.
- si vous configurez l'interface de gestion en tant qu'interface individuelle, vous ne pouvez pas activer le routage dynamique pour l'interface de gestion. Vous devez utiliser une route statique.

Procédure

Étape 1 Affichez toute configuration incompatible afin de pouvoir forcer le mode d'interface et corriger votre configuration ultérieurement; le mode n'est pas modifié avec cette commande :

cluster interface-mode spanned check-details

Exemple :

```
ciscoasa(config)# cluster interface-mode spanned check-details
```

Étape 2 Définissez le mode d'interface pour la mise en grappe :

cluster interface-mode spanned force

Exemple :

```
ciscoasa(config)# cluster interface-mode spanned force
```

Il n'y a pas de paramètres par défaut; vous devez choisir explicitement le mode. Si vous n'avez pas défini le mode, vous ne pouvez pas activer la mise en grappe.

L'option **force** change le mode sans vérifier si votre configuration comporte des paramètres incompatibles. Vous devez résoudre manuellement tous les problèmes de configuration après avoir changé de mode. Étant donné que toute configuration d'interface ne peut être corrigée qu'après avoir défini le mode, nous vous conseillons d'utiliser l'option **force** afin de pouvoir au moins partir de la configuration existante. Vous pouvez réexécuter l'option **check-details** après avoir défini le mode pour obtenir plus de conseils.

Sans l'option **force**, en cas de configuration incompatible, vous êtes invité à effacer votre configuration et à la recharger, ce qui vous obligera à vous connecter au port de console pour reconfigurer votre accès de gestion. Si votre configuration est compatible (ce qui est rare), le mode est modifié et la configuration est conservée. Si vous ne souhaitez pas effacer votre configuration, vous pouvez quitter la commande en tapant **n**.

Pour supprimer le mode d'interface, saisissez la commande **no cluster interface-mode**.

Configurer les interfaces sur le nœud de contrôle

Vous devez modifier toute interface actuellement configurée avec une adresse IP pour qu'elle soit prête pour la grappe avant d'activer la mise en grappe. Pour les autres interfaces, vous pouvez les configurer avant ou après avoir activé la mise en grappe; nous vous recommandons de préconfigurer toutes vos interfaces afin que la configuration complète soit synchronisée avec les nouveaux membres de la grappe.

Cette section décrit comment configurer les interfaces pour qu'elles soient compatibles avec la mise en grappe.

Configurer l'interface de gestion en tant qu'interface individuelle

Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre adresse IP prise dans un ensemble d'adresses IP. L'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle.

nous conseillons de configurer l'interface de gestion en tant qu'interface individuelle. Les interfaces de gestion individuelles vous permettent de vous connecter directement à chaque unité si nécessaire, tandis qu'une interface EtherChannel étendue permet uniquement la connexion au nœud de contrôle.

Avant de commencer

- Pour le mode de contexte multiple, effectuez cette procédure dans chaque contexte. SI vous n'êtes pas déjà en mode de configuration du contexte, saisissez la commande **changeto context** *name*.
- (Facultatif) Configurez l'interface en tant qu'interface EtherChannel locale du périphérique et/ou configurez les sous-interfaces.
  - Dans le cas d'un EtherChannel, celui-ci est local à l'unité et n'est pas un EtherChannel étendu.

Procédure

Étape 1 Configurez un ensemble d'adresses IP locales (IPv4 et/ou IPv6), dont une sera affectée à chaque unité de grappe pour l'interface :

(IPv4)

ip local pool *poolname first-address — last-address* [**mask** *mask*]

(IPv6)

ipv6 local pool *poolname ipv6-address*/*prefix-length number_of_addresses*

Exemple :

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8:45:1002/64 8
```

Incluez au moins autant d'adresses qu'il y a d'unités dans la grappe. Si vous prévoyez d'étendre la grappe, incluez des adresses supplémentaires. L'adresse IP principale de la grappe qui appartient à l'unité principale

actuelle ne fait *pas* partie de cet ensemble; assurez-vous de réserver une adresse IP sur le même réseau pour l'adresse IP principale de la grappe.

Vous ne pouvez pas déterminer à l'avance l'adresse locale exacte attribuée à chaque unité; pour voir l'adresse utilisée sur chaque unité, saisissez la commande **show ip**[**v6**] **local pool** *poolname*. Chaque membre de la grappe se voit attribuer un ID de membre lorsqu'il rejoint la grappe. L'ID détermine l'adresse IP locale utilisée à partir de l'ensemble.

Étape 2 Entrez le mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface management 1/1
```

Étape 3 Définissez l'interface en mode gestion uniquement afin qu'elle ne transmette pas de trafic :

management-only

Par défaut, les interfaces de type de gestion sont configurées en tant que gestion uniquement. En mode transparent, cette commande est toujours activée pour une interface de type de gestion.

Étape 4 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif management
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur.

Étape 5 Définissez l'adresse IP principale de la grappe et identifiez l'ensemble de grappes :

(IPv4)

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

(IPv6)

ipv6 address *ipv6-address*/*prefix-length* **cluster-pool** *poolname*

Exemple :

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8:45:1002::99/64 cluster-pool insipv6
```

Cette adresse IP doit être sur le même réseau que les adresses de l'ensemble d'adresses de la grappe, mais ne doit pas faire partie de ce dernier. Vous pouvez configurer une adresse IPv4 et/ou une adresse IPv6.

Les configurations automatiques DHCP, PPPoE et IPv6 ne sont pas prises en charge; vous devez configurer manuellement les adresses IP. La configuration manuelle de l'adresse Link-Local n'est pas non plus prise en charge.

Étape 6 Définissez le niveau de sécurité, où *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé) :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 100
```

Étape 7 Activez l'interface :

no shutdown

Exemples

L'exemple suivant configure les interfaces Ethernet 1/3 et Ethernet 1/4 en tant qu'EtherChannel local d'appareil, puis configurent l'EtherChannel en tant qu'interface individuelle :

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface ethernet 1/3
channel-group 1 mode active
no shutdown

interface ethernet 1/4
channel-group 1 mode active
no shutdown

interface port-channel 1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8:45:1002::99/64 cluster-pool mgmtipv6
security-level 100
management-only
```

Configurer des EtherChannel étendus

Un EtherChannel étendu couvre tous les ASA de la grappe et assure l'équilibrage de charges dans le cadre de l'opération EtherChannel.

Avant de commencer

- Vous devez être en mode d'interface EtherChannel étendu.
- Pour le mode de contexte multiple, commencez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.
- Pour le mode transparent, configurez le groupe de ponts. Voir Configurer la BVI (Bridge Virtual Interface), à la page 772.
- Lorsque vous utilisez des EtherChannels étendus, l'interface du canal de port ne s'affiche pas tant que la mise en grappe n'est pas complètement activée. Cette exigence empêche le trafic d'être transféré vers une unité qui n'est pas une unité active dans la grappe.

Procédure

Étape 1 Spécifiez l'interface que vous souhaitez ajouter au groupe de canaux :

interface *physical_interface*

Exemple :

```
ciscoasa(config)# interface ethernet 1/1
```

L'ID *physical_interface* comprend le type, le logement et le numéro de port sous la forme type slot/port. Cette première interface du groupe de canaux détermine le type et la vitesse de toutes les autres interfaces du groupe.

Étape 2 Affectez cette interface à un EtherChannel :

channel-group *channel_id* **mode active**

Exemple :

```
ciscoasa(config-if)# channel-group 1 mode active
```

Le *channel_id* est compris entre 1 et 48. Si l'interface de canal de port pour cet ID de canal n'existe pas encore dans la configuration, elle sera ajoutée automatiquement :

interface port-channel *channel_id*

Seul le mode **actif** est pris en charge pour les EtherChannels étendus.

Étape 3 Activez l'interface :

no shutdown

Étape 4 (Facultatif) Ajoutez des interfaces supplémentaires à l'EtherChannel en répétant le processus.

Exemple :

```
ciscoasa(config)# interface ethernet 1/2
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# no shutdown
```

Les interfaces multiples dans l'EtherChannel par unité sont utiles pour se connecter à des commutateurs dans un VSS, vPC, StackWise ou StackWise Virtual.

Étape 5 Spécifiez l'interface de canal de port :

interface port-channel *channel_id*

Exemple :

```
ciscoasa(config)# interface port-channel 1
```

Cette interface a été créée automatiquement lorsque vous avez ajouté une interface au groupe de canaux.

Étape 6 (Facultatif) Si vous créez des sous-interfaces VLAN sur cet EtherChannel, faites-le maintenant.

Exemple :

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

Le reste de cette procédure s'applique aux sous-interfaces.

Étape 7 (Mode de contexte multiple) Affectez l'interface à un contexte. Saisissez ensuite :

changeto context *name*
interface port-channel *channel_id*

Exemple :

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

Pour le mode de contexte multiple, le reste de la configuration d'interface se produit dans chaque contexte.

Étape 8 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif inside
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur.

Étape 9 Effectuez l'une des opérations suivantes, selon le mode de pare-feu.

- Mode routé : définissez l'adresse IPv4 et/ou IPv6 :

  (IPv4)

  ip address *ip_address* [*mask*]

  (IPv6)

  ipv6 address *ipv6-prefix*/*prefix-length*

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

  Les configurations automatiques DHCP, PPPoE et IPv6 ne sont pas prises en charge. Pour les connexions point à point, vous pouvez spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. La configuration manuelle de l'adresse Link-Local n'est pas non plus prise en charge.

- Mode transparent : affectez l'interface à un groupe de ponts :

  bridge-group *number*

Exemple :

```
ciscoasa(config-if)# bridge-group 1
```

Où *le nombre* est un entier compris entre 1 et 100. Vous pouvez attribuer jusqu'à 64 interfaces à un groupe de ponts. Vous ne pouvez pas attribuer la même interface à plusieurs groupes de ponts. Notez que la configuration des BVI comprend l'adresse IP.

Étape 10 Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Où *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 11 Configurez une adresse MAC globale unique et manuelle pour un EtherChannel étendu afin d'éviter d'éventuels problèmes de connectivité au réseau.

mac-address *mac_address*

Exemple :

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

Vous devez configurer une adresse MAC unique qui n'est pas utilisée actuellement sur votre réseau. Dans le cas d'une adresse MAC configurée manuellement, l'adresse MAC reste celle de l'unité de contrôle actuelle. Si vous ne configurez pas d'adresse MAC, si l'unité de contrôle change, la nouvelle unité de contrôle utilisera une nouvelle adresse MAC pour l'interface, ce qui peut provoquer une panne temporaire du réseau.

En mode de contexte multiple, si vous partagez une interface entre les contextes, vous devez plutôt activer la génération automatique des adresses MAC pour ne pas avoir à définir l'adresse MAC manuellement. Notez que vous devez configurer manuellement l'adresse MAC à l'aide de cette commande pour les interfaces *non partagées*.

La *mac_address* est au format H.H.H., où H est une valeur hexadécimale de 16 bits. Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE est saisie comme suit : 000C.F142.4CDE.

Les deux premiers octets d'une adresse MAC manuelle ne peuvent pas être A2 si vous souhaitez également utiliser des adresses MAC générées automatiquement.

Étape 12 (Mode routé) Pour la mise en grappe inter-sites, configurez une adresse MAC et une adresse IP spécifiques au site pour chaque site :

mac-address *mac_address* **site-id** *number* **site-ip** *ip_address*

Exemple :

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

Les adresses IP spécifiques au site doivent se trouver sur le même sous-réseau que l'adresse IP globale. L'adresse MAC spécifique au site et l'adresse IP utilisées par une unité dépendent de l'ID de site que vous spécifiez dans la configuration de démarrage de chaque unité.

Créer la configuration de démarrage

Chaque nœud de la grappe nécessite une configuration de démarrage pour rejoindre la grappe.

Configurer les paramètres de démarrage du nœud de contrôle

Chaque nœud de la grappe nécessite une configuration de démarrage pour rejoindre la grappe. En règle générale, le premier nœud que vous configurez pour rejoindre la grappe sera le nœud de contrôle. Après avoir activé la mise en grappe, après une période de sélection, la grappe choisit un nœud de contrôle. Avec un seul nœud dans la grappe au départ, ce nœud deviendra le nœud de contrôle. Les nœuds que vous ajouterez ensuite à la grappe seront des nœuds de données.

Avant de commencer

- Sauvegardez vos configurations au cas où vous souhaiteriez quitter la grappe ultérieurement et deviez restaurer votre configuration.
- Pour le mode de contexte multiple, effectuez ces procédures dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.
- Vous devez utiliser le port de console pour activer ou désactiver la mise en grappe. Vous ne pouvez pas utiliser Telnet ou SSH.
- Lorsque vous ajoutez un nœud à une grappe en cours d'exécution, il se peut que vous constatiez des interruptions temporaires et limitées de paquets/connexions; c'est un comportement prévu.
- Déterminez à l'avance la taille de la liaison de commande de grappe. Consultez Dimensionner la liaison de commande de grappe, à la page 366.

Procédure

Étape 1 Activez l'interface de liaison de commande de grappe avant de rejoindre la grappe.

Vous identifierez ultérieurement cette interface comme la liaison de commande de grappe lorsque vous activerez la mise en grappe.

Nous vous conseillons de combiner plusieurs interfaces de liaison de commande de grappe dans un EtherChannel si vous avez suffisamment d'interfaces. L'EtherChannel est local à l'ASA et n'est pas un EtherChannel étendu.

La configuration de l'interface de liaison de commande de grappe n'est pas répliquée du nœud de contrôle aux nœuds de données; cependant, vous devez utiliser la même configuration sur chaque nœud. Comme cette configuration n'est pas répliquée, vous devez configurer les interfaces de liaison de commande de grappe séparément sur chaque nœud.

- Vous ne pouvez pas utiliser une sous-interface VLAN comme liaison de commande de grappe.

- Vous ne pouvez pas utiliser une interface de gestion Management *x*/*x* comme liaison de commande de grappe, seule ou en tant qu'EtherChannel.

a) Entrez le mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface ethernet 1/6
```

b) (Facultatif, pour un EtherChannel) Affectez cette interface physique à un EtherChannel :

channel-group *channel_id* **mode on**

Exemple :

```
ciscoasa(config-if)# channel-group 1 mode on
```

Le *channel_id* est compris entre 1 et 48. Si l'interface de canal de port pour cet ID de canal n'existe pas encore dans la configuration, elle sera ajoutée automatiquement :

interface port-channel *channel_id*

Nous vous conseillons d'utiliser le mode activé pour les interfaces membres de la liaison de commande de grappe afin de réduire le trafic inutile sur la liaison de commande de grappe. La liaison de commande de grappe n'a pas besoin du surdébit du trafic LACP, car il s'agit d'un réseau isolé et stable. **Remarque :** nous vous recommandons de régler les EtherChannels de *données* en mode actif.

c) Activez l'interface :

no shutdown

Il vous suffit d'activer l'interface; ne configurez pas de nom pour l'interface ni d'autres paramètres.

d) (Pour un EtherChannel) Répétez l'opération pour chaque interface supplémentaire que vous souhaitez ajouter à l'EtherChannel :

Exemple :

```
ciscoasa(config)# interface ethernet 1/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

Étape 2 Spécifiez le nœud de transfert maximal de l'interface de liaison de commande de grappe, qui doit être supérieur d'au moins 100 octets à la MTU la plus élevée des interfaces de données.

mtu cluster *bytes*

Exemple :

```
ciscoasa(config)# mtu cluster 9198
```

Définissez la MTU entre 1 400 et 9 198 octets, mais pas entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille MTU n'est pas optimale pour le fonctionnement du système. Par défaut, la MTU est de 1500 octets. Nous vous suggérons de régler la MTU de liaison de commande de grappe au maximum de .

Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe.

Par exemple, comme la MTU maximale est de 9198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9098, tandis que la liaison de commande de grappe peut être définie sur 9198.

Cette commande est une commande de configuration globale, mais fait également partie de la configuration de démarrage qui n'est pas répliquée entre les nœuds.

Étape 3 Nommez la grappe et passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Le nom doit être une chaîne ASCII comptant de 1 à 38 caractères. Vous ne pouvez configurer qu'un seul groupe de grappes par nœud. Tous les membres de la grappe doivent utiliser le même nom.

Étape 4 Nommez ce membre de la grappe :

local-unit *unit_name*

Utilisez une chaîne ASCII unique de 1 à 38 caractères. Chaque nœud doit avoir un nom unique. Un nœud ayant un nom en double ne sera pas autorisé dans la grappe.

Exemple :

```
ciscoasa(cfg-cluster)# local-unit node1
```

Étape 5 Spécifiez l'interface de liaison de commande de grappe, de préférence un EtherChannel :

cluster-interface *interface_id* **ip** *ip_address mask*

Exemple :

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

Les sous-interfaces et les interfaces de gestion ne sont pas autorisées.

Spécifiez une adresse IPv4 pour l'adresse IP; IPv6 n'est pas pris en charge pour cette interface. Cette interface ne peut pas avoir de **nameif** configuré.

Pour chaque nœud, spécifiez une adresse IP différente sur le même réseau.

Étape 6 Si vous utilisez la mise en grappe inter-sites, définissez l'ID de site pour ce nœud afin qu'il utilise une adresse MAC propre au site :

site-id *number*

Exemple :

```
ciscoasa(cfg-cluster)# site-id 1
```

Le *nombre* est compris entre 1 et 8.

Étape 7 Définissez la priorité de ce nœud pour les sélections de nœud de contrôle :

priority *priority_number*

Exemple :

```
ciscoasa(cfg-cluster)# priority 1
```

La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée.

Étape 8 (Facultatif) Définissez une clé d'authentification pour le trafic de contrôle sur la liaison de commande de grappe :

key *shared_secret*

Exemple :

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le code secret partagé est utilisé pour générer la clé de chiffrement. Cette commande n'influe pas sur le trafic du chemin de données, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair.

Étape 9 (Facultatif) Spécifiez manuellement l'ID système cLACP et la priorité du système :

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

Exemple :

```
ciscoasa(cfg-cluster)# clacp system-mac 000a.0000.aaaa
```

Lorsqu'il utilise des EtherChannels étendus, l'ASA utilise cLACP pour négocier l'EtherChannel avec le commutateur voisin. Les ASA d'une grappe collaborent à la négociation du cLACP afin qu'ils apparaissent comme un seul périphérique (virtuel) pour le commutateur. Un paramètre de négociation cLACP est un ID système, qui se présente sous la forme d'une adresse MAC. Tous les ASA de la grappe utilisent le même ID système : généré automatiquement par le nœud de contrôle (par défaut) et répliqué sur toutes les unités secondaires; ou spécifié manuellement dans cette commande sous le format *H.H.H*, où H est un chiffre hexadécimal de 16 bits. (Par exemple, l'adresse MAC 00-0A-00-00-AA-AA est saisie sous la forme 000A.0000.AAAA.) Vous souhaiterez peut-être configurer manuellement l'adresse MAC à des fins de dépannage, par exemple, afin de pouvoir utiliser une adresse MAC facilement identifiée. Généralement, vous utilisez l'adresse MAC générée automatiquement.

La priorité du système, comprise entre 1 et 65 535, est utilisée pour déterminer quel nœud est chargé de prendre une décision de regroupement. Par défaut, l'ASA utilise la priorité 1, qui est la priorité la plus élevée. La priorité doit être supérieure à celle du commutateur.

Cette commande ne fait pas partie de la configuration de démarrage, et est répliquée du nœud de contrôle aux nœuds de données. Cependant, vous ne pouvez pas modifier cette valeur après avoir activé la mise en grappe.

Étape 10 Activez la mise en grappe :

enable [**noconfirm**]

Exemple :

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
```

```
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

Lorsque vous saisissez la commande **enable**, l'ASA analyse la configuration en cours d'exécution à la recherche de commandes incompatibles, en vue de cerner des fonctionnalités qui ne sont pas prises en charge avec la grappe, y compris les commandes pouvant être présentes dans la configuration par défaut. Vous êtes invité à supprimer les commandes incompatibles. Si vous répondez **No** (Non), la mise en grappe n'est pas activée. Utilisez le mot clé **noconfirm** pour contourner la confirmation et supprimer automatiquement les commandes incompatibles.

Pour le premier nœud activé, une sélection de nœud de contrôle se produit. Comme le premier nœud doit être le seul membre de la grappe jusqu'à présent, il deviendra le nœud de contrôle. N'effectuez aucune modification de configuration pendant cette période.

Pour désactiver la mise en grappe, saisissez la commande **no enable**.

Remarque
Si vous désactivez la mise en grappe, toutes les interfaces de données sont fermées et seule l'interface de gestion uniquement est active.

Exemples

Dans l'exemple suivant, une interface de gestion est configurée, un EtherChannel local à un périphérique pour la liaison de commande de grappe, puis active la mise en grappe pour l'ASA appelé « node1 », qui deviendra le nœud de contrôle parce qu'il sera ajouté en premier à la grappe :

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8
interface management 1/1
   nameif management
   ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
   ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
   security-level 100
   management-only
   no shutdown

interface ethernet 1/6
   channel-group 1 mode on
   no shutdown

interface ethernet 1/7
   channel-group 1 mode on
   no shutdown

cluster group pod1
   local-unit node1
   cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
```

```
priority 1
key chuntheunavoidable
enable noconfirm
```

Configurer les paramètres de démarrage du nœud de données

Exécutez la procédure suivante pour configurer les nœuds de données.

Avant de commencer

- Vous devez utiliser le port de console pour activer ou désactiver la mise en grappe. Vous ne pouvez pas utiliser Telnet ou SSH.
- Sauvegardez vos configurations au cas où vous souhaiteriez quitter la grappe ultérieurement et deviez restaurer votre configuration.
- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.
- Si vous avez des interfaces dans votre configuration qui n'ont pas été configurées pour la mise en grappe (par exemple, l'interface de gestion Management 1/1 de configuration par défaut), vous pouvez rejoindre la grappe en tant que nœud de données (sans possibilité de devenir le nœud de contrôle dans une sélection actuelle).
- Lorsque vous ajoutez un nœud à une grappe en cours d'exécution, il se peut que vous constatiez des interruptions temporaires et limitées de paquets/connexions; c'est un comportement prévu.

Procédure

Étape 1 Configurez la même interface de liaison de commande de grappe que celle que vous avez configurée pour le nœud de contrôle.

Exemple :

```
ciscoasa(config)# interface ethernet 1/6
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
ciscoasa(config)# interface ethernet 1/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

Étape 2 Spécifiez la même MTU que vous avez configurée pour le nœud de contrôle :

Exemple :

```
ciscoasa(config)# mtu cluster 9198
```

Étape 3 Saisissez le même nom de grappe que celui que vous avez configuré pour le nœud de contrôle :

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 4 Nommez ce membre de la grappe avec une chaîne unique :

local-unit *unit_name*

Exemple :

```
ciscoasa(cfg-cluster)# local-unit node2
```

Spécifiez une chaîne ASCII de 1 à 38 caractères.

Chaque nœud doit avoir un nom unique. Un nœud ayant un nom en double ne sera pas autorisé dans la grappe.

Étape 5 Spécifiez la même interface de liaison de commande de grappe que vous avez configurée pour le nœud de contrôle, mais spécifiez une adresse IP différente sur le même réseau pour chaque nœud :

cluster-interface *interface_id* **ip** *ip_address mask*

Exemple :

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

Spécifiez une adresse IPv4 pour l'adresse IP; IPv6 n'est pas pris en charge pour cette interface. Cette interface ne peut pas avoir de **nameif** configuré.

Étape 6 Si vous utilisez la mise en grappe inter-sites, définissez l'ID de site pour ce nœud afin qu'il utilise une adresse MAC propre au site :

site-id *number*

Exemple :

```
ciscoasa(cfg-cluster)# site-id 1
```

Le **number** est compris entre 1 et 8.

Étape 7 Définissez la priorité de ce nœud pour les sélections de nœuds de contrôle, généralement à une valeur plus élevée que celle du nœud de contrôle :

priority *priority_number*

Exemple :

```
ciscoasa(cfg-cluster)# priority 2
```

Définissez la priorité entre 1 et 100, 1 représentant la priorité la plus élevée.

Étape 8 Définissez la même clé d'authentification que vous avez définie pour le nœud de contrôle :

Exemple :

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

Étape 9 Activez la mise en grappe :

enable as-data-node

Vous pouvez éviter toute incompatibilité de configuration (principalement l'existence d'interfaces non encore configurées pour la mise en grappe) en utilisant la commande **enable as-data-node**. Cette commande garantit que le nœud de données rejoint la grappe sans possibilité de devenir le nœud de contrôle dans une sélection actuelle. Sa configuration est remplacée par celle synchronisée à partir du nœud de contrôle.

Pour désactiver la mise en grappe, saisissez la commande **no enable**.

Remarque
Si vous désactivez la mise en grappe, toutes les interfaces de données sont fermées et seule l'interface de gestion est active.

Exemples

L'exemple suivant comprend la configuration d'un nœud de données, le nœud2 :

```
interface ethernet 1/6

channel-group 1 mode on
no shutdown

interface ethernet 1/7

channel-group 1 mode on
no shutdown

cluster group pod1

local-unit node2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-data-node
```

Personnaliser l'opération de mise en grappe

Vous pouvez personnaliser la surveillance de l'intégrité de la mise en grappe, le délai de réplication de la connexion TCP, la mobilité des flux et d'autres optimisations.

Exécutez ces procédures sur le nœud de contrôle.

Configurer les paramètres de grappe ASA de base

Vous pouvez personnaliser les paramètres de grappe sur le nœud de contrôle.

Avant de commencer

- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système sur le nœud de contrôle. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Étape 2 (Facultatif) Activez la réplication de la console des nœuds de données vers le nœud de contrôle :

console-replicate

Par défaut, cette fonction est désactivée. L'ASA imprime certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de la console, les nœuds de données envoient les messages de la console au nœud de contrôle de sorte que vous ne devez surveiller qu'un seul port de console pour la grappe.

Étape 3 Définissez le niveau de trace minimal pour les événements de mise en grappe :

trace-level *level*

Définissez le niveau minimum comme souhaité :

- **critical**—Événements critiques (gravité=1)
- **warning**—Avertissements (gravité=2)
- **informational**—Événements informationnels (gravité=3)
- **debug**—Événements de débogage (gravité= 4)

Configurer les paramètres de surveillance de l'intégrité et de jonction automatique

Cette procédure permet de configurer la surveillance de l'intégrité des nœuds et des interfaces.

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. Vous pouvez superviser n'importe quel ID de canal de port, ID redondant ou ID d'interface physique unique. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Entrez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

Étape 2 Personnalisez la fonctionnalité de contrôle de l'intégrité des nœuds de la grappe.

health-check [**holdtime** *timeout*] [**vss-enabled**]

Pour déterminer l'intégrité des nœuds, les nœuds de la grappe ASA envoient des messages heartbeat keepaliveheartbeat sur la liaison de commande de grappe aux autres nœuds. Si un nœud ne reçoit pas de messages heartbeat d'un nœud homologue pendant la période d'attente, le nœud homologue est considéré comme non réactif ou mort.

- **holdtime** *timeout* : détermine l'intervalle de temps entre les messages d'état heartbeat des nœuds, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes.
- **vss-enabled** : envoie des messages heartbeat sur toutes les interfaces EtherChannel dans la liaison de commande de grappe pour s'assurer qu'au moins l'un des commutateurs peut les recevoir. Si vous configurez la liaison de commande de grappe en tant EtherChannel (conseillé) et qu'elle est connectée à une paire VSS, vPC, StackWise ou StackWise Virtual, vous devrez peut-être activer l'option **vss-enabled**. Pour certains commutateurs, lorsqu'un nœud du système redondant s'arrête ou démarre, les interfaces membres d'EtherChannel connectées à ce commutateur peuvent sembler être en ligne avec l'ASA, mais elles ne font pas passer de trafic du côté du commutateur. L'ASA peut être supprimé par erreur de la grappe si vous définissez le délai d'attente ASA selon une faible valeur (par exemple 0,8 seconde) et qu'il envoie des messages keepalive sur l'une de ces interfaces EtherChannel.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées (**no health-check monitor-interface**). Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver le contrôle d'intégrité.

Exemple :

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

Étape 3 Désactivez le contrôle d'intégrité de l'interface sur une interface.

no health-check monitor-interface *interface_id*

La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que l'ASA ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit un membre établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces. Vous pouvez le désactiver pour chaque interface en utilisant la forme **no** (non) de cette commande. Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion.

- *interface_id* : désactive la surveillance de tout ID de canal de port, ID redondant ou ID d'interface physique unique. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité (**no health-check**) et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque

la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver le contrôle d'intégrité.

Exemple :

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

Étape 4 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system** : spécifie les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.
- **unlimited** : (Par défaut pour le **cluster-interface**) Ne limite pas le nombre de tentatives de jonction.
- *auto-rejoin-max* : définit le nombre de tentatives de jonction, entre 0 et 65535. **0** désactive la jonction automatique. La valeur par défaut pour les commandes **data-interface** et **system** est de 3.
- *auto_rejoin_interval* : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- *auto_rejoin_interval_variation* : définit si la durée de l'intervalle augmente. Définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données et le système

Exemple :

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

Étape 5 Configurez le délai antirebond avant que l'ASA considère une interface comme défaillante et que le nœud ne soit supprimé de la grappe.

health-check monitor-interface debounce-time *ms*

Exemple :

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

Définissez le délai antirebond entre 300 et 9 000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe d'un état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un délai antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe simplement parce qu'un autre nœud de la grappe a été plus rapide à regrouper les ports.

Étape 6 (Facultatif) Configurez la surveillance de la charge de trafic.

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* : définit le délai en secondes entre les messages de surveillance, entre 10 et 360 secondes. La valeur par défaut est de 20 secondes.
- **intervals** *intervals* : définit le nombre d'intervalles pour lesquels l'ASA conserve les données, entre 1 et 60. La valeur par défaut est 30.

Vous pouvez superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud si les nœuds restants peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Par exemple, pour la mise en grappe inter-châssis sur le Firepower 9300 avec 3 modules de sécurité dans chaque châssis, si deux modules de sécurité d'un châssis quittent la grappe, la même quantité de trafic vers le châssis sera envoyée au module restant et risque de le submerger. Vous pouvez superviser périodiquement la charge de trafic. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud.

Utilisez la commande **show cluster info load-monitor** pour afficher la charge de trafic.

Exemple :

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

Exemple

L'exemple suivant configure le délai de rétention du contrôle d'intégrité à 0,3 seconde; active VSS; désactive la surveillance sur l'interface Ethernet 1/2, qui est utilisée pour la gestion; définit la reconnexion automatique pour les interfaces de données à 4 tentatives commençant à 2 minutes, en multipliant la durée de 3 fois l'intervalle précédent; et définit la reconnexion automatique pour la liaison de commande de grappe à 6 tentatives toutes les 2 minutes.

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3 vss-enabled
ciscoasa(cfg-cluster)# no health-check monitor-interface ethernet1/2
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

Configurer la rééquilibrage de la connexion et le délai de réplication TCP de la grappe

Vous pouvez configurer le rééquilibrage des connexions. Pour en savoir plus, consultez Rééquilibrage des nouvelles connexions TCP dans la grappe, à la page 444

Activez le délai de réplication de la grappe pour les connexions TCP pour aider à éliminer le « travail inutile » lié aux flux de courte durée en retardant la création du flux directeur/de sauvegarde. Notez que si un nœud tombe en panne avant la création du flux directeur/de sauvegarde, ces flux ne peuvent pas être récupérés. De même, si le trafic est rééquilibré vers un autre nœud avant la création du flux, le flux ne peut pas être récupéré. Vous ne devez pas activer la réplication TCP pour le trafic sur lequel vous désactivez la répartition aléatoire TCP.

Procédure

Étape 1 Activez le délai de réplication de la grappe pour les connexions TCP :

cluster replication delay *seconds* {**http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] {**host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

Exemple :

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

Définissez les *secondes* entre 1 et 15. Le délai **http** est activé par défaut pendant 5 secondes.

En mode de contexte multiple, configurez ce paramètre dans le contexte.

Étape 2 Entrez en mode de configuration de la grappe :

cluster group *name*

Étape 3 (Facultatif) Activez le rééquilibrage des connexions pour le trafic TCP :

conn-rebalance [**frequency** *seconds*]

Exemple :

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

Cette commande est désactivée par défaut. Si cette option est activée, les ASA échangent périodiquement des renseignements sur les connexions par seconde et déchargent les nouvelles connexions des appareils ayant plus de connexions par seconde vers les appareils moins chargés. Les connexions existantes ne sont jamais déplacées. De plus, comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées. La valeur par défaut est de 5 secondes.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Configurer les fonctionnalités inter-sites

Pour la mise en grappe inter-sites, vous pouvez personnaliser votre configuration pour améliorer la redondance et la stabilité.

Activer la localisation du directeur

Pour améliorer les performances et réduire la latence d'aller-retour dans le cas de la mise en grappe inter-sites pour les centres de données, vous pouvez activer la localisation du directeur. Les nouvelles connexions sont généralement équilibrées et appartiennent aux membres de la grappe d'un site donné. Cependant, l'ASA attribue le rôle de directeur à un membre sur *n'importe quel* site. La localisation du directeur permet des rôles de directeur supplémentaires : un directeur local sur le même site que le propriétaire et un directeur global qui peut se trouver sur n'importe quel site. Le fait de maintenir le propriétaire et le directeur sur le même site améliore les performances. En cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site. Le directeur global est utilisé si un membre d'une grappe reçoit des paquets pour une connexion appartenant à un autre site.

Avant de commencer

- Définissez l'ID de site pour le membre de la grappe dans la configuration de démarrage.
- Les types de trafic suivants ne prennent pas en charge la localisation : trafic NAT ou PAT; trafic inspecté par SCTP; requête du propriétaire de la fragmentation.

Procédure

Étape 1 Entrez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

Étape 2 Activez la localisation du directeur.

director-localization

Activer la redondance de site

Pour protéger les flux contre une défaillance de site, vous pouvez activer la redondance de site. Si le propriétaire de connexion de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site.

Avant de commencer

- Définissez l'ID de site pour le membre de la grappe dans la configuration de démarrage.

Procédure

Étape 1 Entrez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

Étape 2 Activez la redondance de site.

site-redundancy

Configurer l'ARP gratuit par site

L'ASA génère maintenant des paquets ARP gratuits (GARP) pour maintenir l'infrastructure de commutation à jour : le membre ayant la priorité la plus élevée sur chaque site génère périodiquement du trafic GARP pour les adresses MAC et IP globales.

Lorsque vous utilisez des adresses MAC et IP par site, les paquets provant de la grappe utilisent une adresse MAC et une adresse IP propres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IP globales. Si le trafic n'est pas généré périodiquement à partir de l'adresse MAC globale, vous pourriez rencontrer un délai d'expiration de l'adresse MAC sur vos commutateurs pour l'adresse MAC globale. Après un délai d'expiration, le trafic destiné à l'adresse MAC globale sera inondé dans l'ensemble de l'infrastructure de commutation, ce qui peut entraîner des problèmes de performance et de sécurité.

Le GARP est activé par défaut lorsque vous définissez l'ID de site pour chaque unité et l'adresse MAC du site pour chaque EtherChannel étendu. Vous pouvez personnaliser l'intervalle GARP ou vous pouvez désactiver GARP.

Avant de commencer

- Définissez l'ID de site pour le membre de la grappe dans la configuration de démarrage.
- Définissez l' adresse MAC par site pour l' EtherChannel étendu dans la configuration de l'unité de contrôle.

Procédure

Étape 1 Entrez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group cluster1
```

```
ciscoasa(cfg-cluster)#
```

Étape 2 Personnalisez l'intervalle GARP.

site-periodic-garp interval *seconds*

- *seconds* :Définissez le temps en secondes entre la génération du GARP, entre 1 et 1000000 secondes. La valeur par défaut est de 290 secondes.

Pour désactiver GARP, saisissez **no site-periodic-garp interval**.

Configurer la mobilité des flux de grappes

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

À propos de l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux entre les sites.

À propos de LISP

La mobilité des machines virtuelles de centres de données, comme VMware VMotion, permet aux serveurs de migrer entre les centres de données tout en maintenant les connexions avec les clients. Pour prendre en charge une telle mobilité de serveur de centre de données, les routeurs doivent être en mesure de mettre à jour la route d'entrée vers le serveur lorsqu'il se déplace. L'architecture Cisco Locator/Protocole de séparation d'ID (LISP) sépare l'identité du périphérique, ou l'identifiant de terminal (EID), de son emplacement, ou localisateur de routage, dans deux espaces de numérotation différents, ce qui rend la migration du serveur transparente pour les clients. Par exemple, lorsqu'un serveur est déplacé vers un nouveau site et qu'un client envoie du trafic vers le serveur, le routeur redirige le trafic vers le nouvel emplacement.

LISP nécessite des routeurs et des serveurs dans certains rôles, tels que le routeur de tunnel de sortie (ETR) LISP, le routeur de tunnel d'entrée (ITR), les routeurs de premier saut, le résolveur de carte (MR) et le serveur de carte (MS). Lorsque le routeur du premier saut du serveur détecte que le serveur est connecté à un autre routeur, il met à jour tous les autres routeurs et les bases de données afin que l'ITR connectée au client puisse intercepter, encapsuler et envoyer le trafic vers le nouvel emplacement du serveur.

Prise en charge du LISP ASA

L'ASA n'exécute pas le LISP lui-même; il peut, cependant, inspecter le trafic LISP pour détecter les changements d'emplacement, puis utiliser ces informations pour un fonctionnement de mise en grappe transparent. Sans l'intégration du LISP, lorsqu'un serveur est déplacé vers un nouveau site, le trafic est acheminé vers un membre de la grappe ASA sur le nouveau site plutôt que vers le propriétaire d'origine du flux. Le nouvel ASA transfère le trafic vers l'ASA au niveau de l'ancien site, puis l'ancien ASA doit renvoyer le trafic vers le nouveau site pour qu'il atteigne le serveur. Ce flux de trafic est sous-optimal et est connu comme « tromboning » ou « épingle à cheveux ».

Grâce à l'intégration du LISP, les membres de la grappe ASA peuvent inspecter le trafic LISP passant entre le routeur du premier saut et l'ETR ou l'ITR, puis peuvent changer le propriétaire du flux pour qu'il se trouve sur le nouveau site.

Lignes directrices LISP

- Les membres de la grappe ASA doivent se trouver entre le routeur du premier saut et l'ITR ou l'ETR du site. La grappe ASA elle-même ne peut pas être le premier routeur de saut pour un segment étendu.
- Seuls les flux entièrement distribués sont pris en charge; les flux centralisés, les flux semi-distribués ou les flux appartenant à des nœuds individuels ne sont pas transférés vers de nouveaux propriétaires. Les flux semi-distribués comprennent des applications, telles que SIP, où tous les flux enfants appartiennent au même ASA qui possède le flux parent.
- La grappe déplace uniquement les états de flux de couche 3 et 4; certaines données d'application pourraient être perdues.
- Pour les flux de courte durée ou non essentiels pour l'entreprise, le déplacement du propriétaire peut ne pas valoir la peine. Vous pouvez contrôler les types de trafic pris en charge avec cette fonctionnalité lorsque vous configurez la politique d'inspection. Vous devez limiter la mobilité de flux au trafic essentiel.

Mise en œuvre du LISP ASA

Cette fonctionnalité comprend plusieurs configurations interdépendantes (qui sont toutes décrites dans ce chapitre) :

1. (Facultatif) Limiter les EID inspectés en fonction de l'adresse IP de l'hôte ou du serveur : le routeur de premier saut pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée, vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.
2. Inspection du trafic LISP : l'ASA inspecte le trafic LISP sur le port UDP 4342 pour détecter le message EID-notify envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui met en corrélation l'EID et l'ID de site. Par exemple, vous devez inspecter le trafic LISP avec une adresse IP source du routeur du premier saut et une adresse de destination de l'ITR ou de l'ETR. Remarque : le trafic LISP n'a pas de directeur affecté et le trafic LISP en lui-même ne participe pas au partage de l'état de la grappe.
3. Politique de service pour activer la mobilité des flux sur le trafic spécifié : vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.
4. ID de sites : l'ASA utilise l'ID de site pour chaque nœud de la grappe afin de déterminer le nouveau propriétaire.
5. Configuration au niveau de la grappe pour activer la mobilité de flux : vous devez également activer la mobilité de flux au niveau de la grappe. Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité de flux pour une classe particulière de trafic ou d'applications.

Configurer l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

Avant de commencer

- Affectez chaque unité de grappe à un ID de site en fonction de Configurer les paramètres de démarrage du nœud de contrôle, à la page 378 et Configurer les paramètres de démarrage du nœud de données, à la page 383.

- Le trafic LISP n'est pas inclus dans la classe de trafic d'inspection par défaut. Vous devez donc configurer une classe distincte pour le trafic LISP dans le cadre de cette procédure.

Procédure

Étape 1 (Facultatif) Configurez une carte d'inspection LISP pour limiter les EID inspectés en fonction de l'adresse IP et pour configurer la clé partagée LISP :

a) Créez une ACL étendue; seule l'adresse IP de destination correspond à l'adresse intégrée de l'EID :

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

Les ACL IPv4 et IPv6 sont acceptées. Consultez la référence de commande pour connaître la syntaxe **access-list extended** exacte.

b) Créez la carte d'inspection LISP et entrez le mode des paramètres :

policy-map type inspect lisp *inspect_map_name*

parameters

c) Définissez les EID autorisés en identifiant l'ACL que vous avez créée :

allowed-eid access-list *eid_acl_name*

Le routeur de premier saut ou l'ITR/ETR pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée; vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.

d) Si nécessaire, saisissez la clé partagée :

validate-key *key*

Exemple :

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

Étape 2 Configurez l'inspection LISP pour le trafic UDP entre le routeur de premier saut et l'ITR ou l'ETR sur le port 4342 :

a) Configurez l'ACL étendue pour identifier le trafic LISP :

access list *inspect_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

Vous *devez* spécifier le port UDP 4342. Les ACL IPv4 et IPv6 sont acceptées. Consultez la référence de commande pour connaître la syntaxe **access-list extended** exacte.

b) Créez une carte de trafic pour l'ACL :

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) Spécifiez la liste des politiques, la carte de trafic, activez l'inspection à l'aide de la carte d'inspection LISP facultative et appliquez la politique de service à une interface (si nouvelle) :

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

Si vous avez une politique de service existante, spécifiez le nom de la liste des politiques existante. Par défaut, l'ASA inlcut une politique globale appelée **global_policy**, donc pour une politique globale, spécifiez ce nom. Vous pouvez également créer une politique de service par interface si vous ne souhaitez pas appliquer la politique à l'échelle mondiale. L'inspection LISP est appliquée au trafic de manière bidirectionnelle, vous n'avez donc pas besoin d'appliquer la politique de service sur les interfaces source et de destination; tout le trafic qui entre ou sort de l'interface à laquelle vous appliquez la liste des politiques est affecté si le trafic correspond à la carte de trafic dans les deux sens.

Exemple :

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

L'ASA inspecte le trafic LISP pour détecter le message de notification d'EID envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui met en corrélation l'EID et l'ID de site.

Étape 3 Activez la mobilité des flux pour une classe de trafic :

a) Configurez l'ACL étendue pour identifier le trafic opérationnel critique que vous souhaitez réaffecter au site le plus optimal lorsque les serveurs changent de site :

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

Les ACL IPv4 et IPv6 sont acceptées. Consultez la référence de commande pour connaître la syntaxe **access-list extended** exacte. Vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.

b) Créez une carte de trafic pour l'ACL :

class-map *flow_map_name*

match access-list *flow_acl_name*

c) Spécifiez la même liste des politiques sur laquelle vous avez activé l'inspection LISP, la carte de trafic de flux, et activez la mobilité des flux :

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

Exemple :

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

Étape 4 Entrez dans le mode de configuration du groupe de grappes et activez la mobilité des flux pour la grappe :

cluster group *name*

flow-mobility lisp

Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité des flux.

Exemples

L'exemple suivant :

- Limite les EID à ceux sur le réseau 10.10.10.0/24
- Inspecte le trafic LISP (UDP 4342) entre un routeur LISP à l'adresse 192.168.50.89 (à l'intérieur) et un routeur ITR ou ETTR (sur une autre interface ASA) à l'adresse 192.168.10.8
- Active la mobilité des flux pour tout le trafic interne vers un serveur sur 10.10.10.0/24 à l'aide de HTTPS.
- Active la mobilité des flux pour la grappe.

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

Gérer les nœuds de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les nœuds de cette dernière.

Devenir un nœud inactif

Pour devenir un membre inactif de la grappe, désactivez la mise en grappe sur le nœud tout en laissant intacte la configuration de mise en grappe.

Remarque Lorsqu'un ASA devient inactif (soit manuellement, soit à la suite d'un échec du contrôle d'intégrité), toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe; ou vous pouvez supprimer complètement le nœud de la grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), alors l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Avant de commencer

- Vous devez utiliser le port de console; vous ne pouvez pas activer ni désactiver la mise en grappe à partir d'une connexion distante d'interface de ligne de commande.
- Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 2 Désactivez la mise en grappe :

no enable

Si ce nœud était le nœud de contrôle, une nouvelle sélection de contrôle a lieu et un autre membre devient le nœud de contrôle.

La configuration de la grappe est conservée, vous pouvez donc réactiver la mise en grappe ultérieurement.

Désactiver undonnées

Pour désactiver un membre autre que le nœud auquel vous êtes connecté, effectuez les étapes suivantes.

Remarque Lorsqu'un ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Avant de commencer

Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.

Procédure

Supprimez le nœud de la grappe.

cluster remove unit *node_name*

La configuration de démarrage reste inchangée, ainsi que la dernière configuration synchronisée à partir du nœud de contrôle, afin que vous puissiez rajouter le nœud ultérieurement sans perdre votre configuration. Si vous saisissez cette commande sur un nœud de données pour supprimer le nœud de contrôle, un nouveau nœud de contrôle est élu.

Pour afficher les noms des membres, saisissez **cluster remove unit ?**, ou saisissez la commande **show cluster info**.

Exemple :

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement un membre, vous devez rejoindre manuellement la grappe.

Avant de commencer

- Vous devez utiliser le port de console pour réactiver la mise en grappe. Les autres interfaces sont fermées.
- Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.
- Assurez-vous que le problème est résolu avant d'essayer de rejoindre la grappe.

Procédure

Étape 1 Sur la console, passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 2 Activez la mise en grappe.

enable

Quitter la grappe

Si vous souhaitez quitter complètement la grappe, vous devez supprimer toute la configuration de démarrage de la grappe. Étant donné que la configuration actuelle sur chaque nœud est la même (synchronisée à partir de l'unité active), quitter la grappe implique également de restaurer une configuration antérieure à la grappe à partir d'une sauvegarde ou d'effacer votre configuration et de recommencer pour éviter les conflits d'adresses IP.

Avant de commencer

Vous devez utiliser le port de console; lorsque vous supprimez la configuration de la grappe, toutes les interfaces sont fermées, y compris l'interface de gestion et la liaison de commande de grappe. De plus, vous ne pouvez pas activer ni désactiver la mise en grappe à partir d'une connexion distante d'interface de ligne de commande.

Procédure

Étape 1 Pour un nœud de données, désactivez la mise en grappe :

cluster group *cluster_name* **no enable**

Exemple :

```
ciscoasa(config)# cluster group cluster1
```

```
ciscoasa(cfg-cluster)# no enable
```

Vous ne pouvez pas modifier la configuration lorsque la mise en grappe est activée sur un nœud de données.

Étape 2 Effacez la configuration de la grappe :

clear configure cluster

L'ASA désactive toutes les interfaces, y compris l'interface de gestion et la liaison de commande de grappe.

Étape 3 Désactivez le mode d'interface de la grappe :

no cluster interface-mode

Le mode n'est pas stocké dans la configuration et doit être réinitialisé manuellement.

Étape 4 Si vous avez une configuration de sauvegarde, copiez-la dans la configuration en cours d'exécution :

copy *backup_cfg* **running-config**

Exemple :

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

Étape 5 Enregistrez la configuration pour le démarrage :

write memory

Étape 6 Si vous n'avez pas de configuration de sauvegarde, reconfigurez l'accès de gestion. Par exemple, assurez-vous de modifier les adresses IP de l'interface et de restaurer le bon nom d'hôte.

Modifier le nœud de contrôle



Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez spécifier le nœud exact que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez toutefois que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle à l'aide de cette procédure, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Avant de commencer

Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.

Procédure

Définissez un nouveau nœud comme nœud de contrôle :

cluster control-node unit*node_name*

Exemple :

```
ciscoasa(config)# cluster control-node unit asa2
```

Vous devrez vous reconnecter à l'adresse IP de la grappe principale.

Pour afficher les noms des membres, saisissez **cluster control-node unit ?** (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exécuter une commande à l'échelle de la grappe

Pour envoyer une commande à tous les nœuds de la grappe ou à un nœud en particulier, procédez comme suit. L'envoi d'une commande **show** à tous les nœuds collecte toutes les sorties et les affiche sur la console du nœud actuel. D'autres commandes, telles que **capture** et **copy**, peuvent également profiter d'une exécution à l'échelle de la grappe.

Procédure

Envoyez une commande à tous les nœuds ou, si vous spécifiez le nom du nœud, à un nœud en particulier :

cluster exec [**unit** *node_name*] *command*

Exemple :

```
ciscoasa# cluster exec show xlate
```

Pour afficher les noms de nœud, saisissez **cluster exec unit ?** (unité d'exécution de grappe?) (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exemples

Pour copier simultanément le même fichier de capture de tous les nœuds de la grappe vers un serveur TFTP, saisissez la commande suivante sur le nœud de contrôle :

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Plusieurs fichiers PCAP, un pour chaque nœud, sont copiés sur le serveur TFTP. Le nom du fichier de capture de destination est automatiquement associé au nom du nœud, par exemple

capture1_asa1.pcap, capture1_asa2.pcap, etc. Dans cet exemple, asa1 et asa2 sont des noms de nœuds de grappe.

L'exemple de sortie suivant pour la commande **cluster exec show port-channel summary** affiche les renseignements de l'EtherChannel pour chaque nœud de la grappe :

```
ciscoasa# cluster exec show port-channel summary
control node(LOCAL):**********************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 slave:***********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

Supervision de la grappe ASA

Vous pouvez superviser et dépanner l'état de la grappe et les connexions.

Supervision de l'état de la grappe

Consultez les commandes suivantes pour superviser l'état de la grappe :

- **show cluster info** [**health** [**details**]]

  En l'absence de mot clé, la commande **show cluster info** affiche l'état de tous les membres de la grappe.

  La commande **show cluster info health** affiche l'intégrité actuelle des interfaces, des nœuds et de la grappe dans son ensemble. Le mot clé **details** affiche le nombre d'échecs de messages de pulsation.

  Consultez la sortie suivante pour la commande **show cluster info** :

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
```

```
    Last join : 19:13:11 UTC Sep 23 2011
    Last leave: N/A
Unit "A" in state CONTROL_NODE
    ID        : 2
    Site ID   : 2
          Version   : 9.4(1)
    Serial No.: JAB0815R0JY
    CCL IP    : 10.0.0.1
    CCL MAC   : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2011
    Last leave: N/A
Unit "B" in state DATA_NODE
    ID        : 3
    Site ID   : 2
          Version   : 9.4(1)
    Serial No.: P3000000191
    CCL IP    : 10.0.0.2
    CCL MAC   : 000b.fcf8.c61e
    Last join : 19:13:50 UTC Sep 23 2011
    Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  Indique si le nœud de la grappe rejoindra automatiquement la grappe après un délai et si les conditions de défaillance (comme l'attente de la licence, l'échec de la vérification de l'intégrité du châssis, etc.) sont supprimées. Si le nœud est désactivé de façon permanente ou si le nœud est déjà dans la grappe, cette commande n'affichera aucune sortie.

  Consultez les sorties suivantes pour la commande **show cluster info auto-join** :

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport** {**asp** | **cp** [**detail**]}

  Affiche les statistiques relatives au transport pour les éléments suivants :

- **asp** – Statistiques de transport du plan de données.
- **cp** – Statistiques de transport du plan de commande.

Si vous saisissez le mot clé **detail**, vous pouvez afficher l'utilisation du protocole de transport fiable de la grappe afin de cerner les problèmes d'abandon de paquet lorsque le tampon est plein dans le plan de commande. Consultez la sortie suivante pour la commande **show cluster info transport cp detail** :

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
--------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
-----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-----------------------------------------------
        0         2         3
  U     1         3308122   4370233
```

```
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  -------------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  -------------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
```

```
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                       578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                       572         99%
  Cluster VPN Unique ID Client                     1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  Affiche l'historique de la grappe, ainsi que les messages d'erreur indiquant pourquoi un nœud de grappe n'a pas pu se joindre ou pourquoi un nœud a quitté a grappe.

Capture des paquets à l'échelle de la grappe

Consultez la commande suivante pour capturer des paquets dans une grappe :

cluster exec capture

Pour prendre en charge le dépannage à l'échelle de la grappe, vous pouvez activer la capture du trafic spécifique à la grappe sur le nœud de contrôle à l'aide de la commande **cluster exec capture**, qui est ensuite automatiquement activée sur tous les nœuds de données de la grappe.

Supervision des ressources de la grappe

Consultez la commande suivante pour surveiller les ressources de la grappe :

show cluster {**cpu** | **memory** | **resource**} [*options*]

Affiche les données agrégées pour l'ensemble de la grappe. Les *options* disponibles dépendent du type de données.

Supervision du trafic de la grappe

Consultez les écrans suivantes pour superviser le trafic de la grappe :

- **show conn [detail], cluster exec show conn**

  La commande **show conn** indique si un flux est un flux de directeur, de sauvegarde ou de transfert. Utilisez la commande **cluster exec show conn** sur n'importe quel nœud pour afficher toutes les connexions. Cette commande peut montrer comment le trafic d'un flux unique arrive à différents ASA dans la grappe. Le débit de la grappe dépend de l'efficacité et de la configuration de l'équilibrage de charges. Cette commande offre un moyen simple d'afficher le trafic d'une connexion dans la grappe et peut vous aider à comprendre comment un équilibreur de charges peut affecter les performances d'un flux.

  La commande **show conn detail** indique également quels flux sont soumis à la mobilité des flux.

  L'exemple suivant illustre une sortie de la commande **show conn detail** :

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic received
 at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface NP
Identity
Ifc Locally received: 716 (8 byte/s)
```

  Pour dépanner le flux de connexion, observez d'abord les connexions sur tous les nœuds en saisissant la commande **cluster exec show conn** sur n'importe quel nœud. Recherchez les flux qui ont les indicateurs suivants : directeur (Y), sauvegarde (y) et transitaire (z). L'exemple suivant montre une connexion SSH de 172.18.124.187:22 à 192.168.103.131:44727 sur les trois ASA; l'ASA 1 a l'indicateur z indiquant qu'il s'agit d'un transitaire pour la connexion, l'ASA 3 a l'indicateur y indiquant qu'il est le directeur

de la connexion et l'ASA 2 n'a pas d'indicateurs spéciaux indiquant qu'il est le propriétaire. Dans le sens sortant, les paquets de cette connexion pénètrent dans l'interface interne de l'ASA 2 et quittent l'interface externe. Dans le sens entrant, les paquets de cette connexion pénètrent dans l'interface externe sur l'ASA 1 et l'ASA 3, sont acheminés sur la liaison de commande de grappe vers l'ASA 2, puis quittent l'interface interne sur l'ASA 2.

```
ciscoasa/ASA1/control node# cluster exec show conn
ASA1(LOCAL):************************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:************************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:************************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  Les commandes **show cluster info conn-distribution** et **show cluster info packet-distribution** affichent la distribution du trafic sur tous les nœuds de la grappe. Ces commandes peuvent vous aider à évaluer et à ajuster l'équilibreur de charges externe.

  La commande **show cluster info loadbalance** affiche les statistiques de rééquilibrage des connexions.

  La commande **show cluster info flow-mobility counters** affiche les renseignements sur le mouvement de l'EID et le mouvement du propriétaire du flux. Consultez la sortie suivante pour **show cluster info flow-mobility counters** :

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  La commande **show cluster info load-monitor** affiche la charge de trafic pour les membres de la grappe pour le dernier intervalle ainsi que la moyenne du nombre total d'intervalles configurés (30 par défaut). Utilisez le mot clé **details** pour afficher la valeur de chaque mesure à chaque intervalle.

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
```

```
Average from last 30 interval:
   0           0           0           12              28
   1           0           0           13              27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval


Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0
```

```
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
         25         20         30         30         30         30
Unit ID  1
         30         25         35         25         30         30
         25         25         35         25         30         35
         30         30         35         30         30         30
         25         20         30         25         25         30
         20         30         35         30         30         35

CPU usage(%) captured over 30 intervals:
Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
         25         20         30         30         30         30
Unit ID  1
         30         25         35         25         30         30
         25         25         35         25         30         35
         30         30         35         30         30         30
         25         20         30         25         25         30
         20         30         35         30         30         35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  Affiche les données agrégées pour l'ensemble de la grappe. Les *options* disponibles dépendent du type de données.

  Consultez la sortie suivante pour la commande **show cluster access-list** :

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

  Pour afficher le nombre agrégé des connexions utilisées pour tous les nœuds, saisissez :

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used

  cl1:************************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  Cette commande est utile pour le dépannage des chemins de données.

Supervision du routage de la grappe

Consultez les commandes suivantes pour le routage de la grappe :

- **show route cluster**
- **debug route cluster**

  Affiche les renseignements sur la grappe pour le routage.

- **show lisp eid**

  Affiche le tableau EID de l'ASA qui indique les EID et les ID de site.

  Consultez la sortie suivante de la commande **cluster exec show lisp eid**.

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):**********************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:**********************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  Cette commande est utile pour la résolution de problèmes.

Configuration de la journalisation pour la mise en grappe

Consultez la commande suivante pour configurer la journalisation pour la mise en grappe :

logging device-id

Chaque nœud de la grappe génère des messages de journal système de manière indépendante. Vous pouvez utiliser la commande **logging device-id** pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant de nœuds identiques ou différents dans la grappe.

Supervision des interfaces de grappe

Consultez les commandes suivantes pour superviser les interfaces de la grappe :

- **show cluster interface-mode**

  Affiche le mode d'interface de la grappe.

- **show port-channel**

  Comprend des renseignements indiquant si un canal de port est étendu.

- **show lacp cluster {system-mac | system-id}**

  Affiche l'ID système et la priorité cLACP.

- **debug lacp cluster [all | ccp | misc | protocol]**

  Affiche les messages de débogage pour cLACP.

- **show interface**

  Affiche l'utilisation de l'adresse MAC du site lorsqu'elle est utilisée :

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
VLAN identifier 3151
MAC address aaaa.1111.1234, MTU 1500
Site Specific MAC address aaaa.1111.aaaa
IP address 10.3.1.1, subnet mask 255.255.255.0
Traffic Statistics for "inside":
132269 packets input, 6483425 bytes
1062 packets output, 110448 bytes
98530 packets dropped
```

Débogage de la mise en grappe

Consultez les commandes suivantes pour le débogage de la mise en grappe :

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  Affiche les messages de débogage pour la mise en grappe.

- **debug cluster flow-mobility**

  Affiche les événements liés à la mobilité des flux de mise en grappe.

- **debug lisp eid-notify-intercept**

  Affiche les événements lorsque le message eid-notify est intercepté.

- **show cluster info trace**

  La commande **show cluster info trace** affiche les renseignements de débogage pour un dépannage ultérieur.

  Consultez la sortie suivante pour la commande **show cluster info trace** :

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

  Par exemple, si vous voyez les messages suivants indiquant que deux nœuds ayant le même nom **local-unit** agissent en tant que nœud de contrôle, cela peut signifier que deux nœuds ont le même nom **local-unit** (vérifiez votre configuration) ou qu'un nœud reçoit ses propres messages de diffusion (vérifiez votre réseau).

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node
 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

Exemples de mise en grappe ASA

Ces exemples incluent toutes les configurations ASA liées aux grappes pour les déploiements typiques.

Exemple de configuration ASA et du commutateur

Les exemples de configuration suivants connectent les interfaces suivantes entre l'ASA et le commutateur :

Interface ASA	Interface du commutateur
Ethernet 1/2	GigabitEthernet 1/0/15
Ethernet 1/3	GigabitEthernet 1/0/16
Ethernet 1/4	GigabitEthernet 1/0/17
Ethernet 1/5	GigabitEthernet 1/0/18

Configuration ASA

Mode d'interface sur chaque unité

```
cluster interface-mode spanned force
```

Configuration de démarrage de l'unité de contrôle ASA1

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
```

```
 priority 10
 key emphyri0
 enable noconfirm
```

Configuration de démarrage de l'unité de données ASA2

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-data-node
```

Configuration de l'interface de l'unité de contrôle

```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface Ethernet1/2
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/3
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/4
 channel-group 11 mode active
 no shutdown
!
interface Ethernet1/5
 channel-group 11 mode active
 no shutdown
!
interface Management1/1
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 mac-address aaaa.dddd.cccc
```

```
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

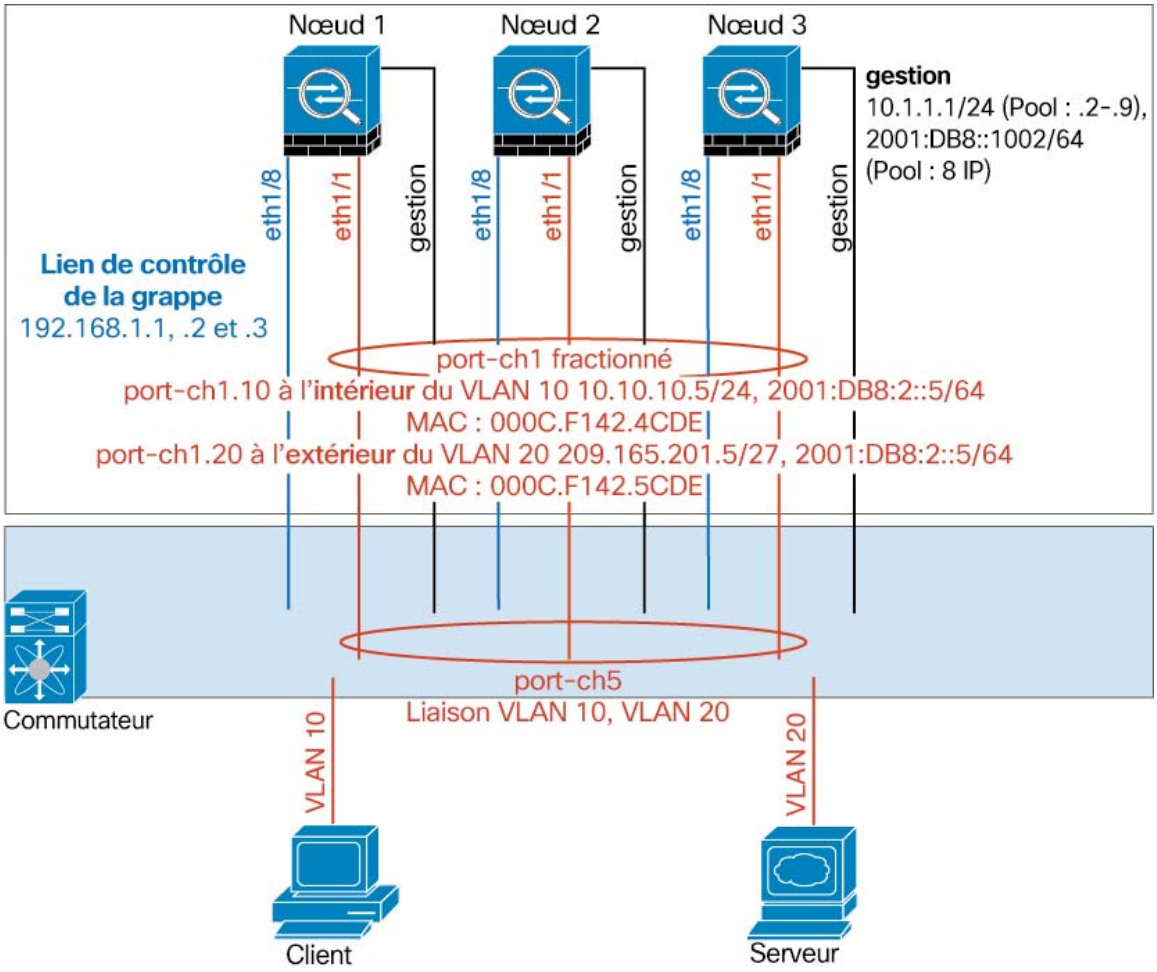
Configuration du commutateur Cisco IOS

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

Pare-feu sur clé



Le trafic de données provenant de différents domaines de sécurité est associé à différents VLAN, par exemple, le VLAN 10 pour le réseau interne et le VLAN 20 pour le réseau externe. Chaque ASA dispose d'un seul port physique connecté au commutateur ou routeur externe. Le regroupement de liaisons est activé de sorte que tous les paquets sur la liaison physique soient encapsulés dans une norme 802.1q. L' ASA sert de pare-feu entre le VLAN 10 et le VLAN 20.

Lorsque vous utilisez des EtherChannels étendus, toutes les liaisons de données sont regroupées dans un seul EtherChannel du côté du commutateur. Si l'ASA n'est plus disponible, le commutateur rééquilibre le trafic entre les unités restantes.

Mode d'interface sur chaque unité

```
cluster interface-mode spanned force
```

Configuration de démarrage de l'unité de contrôle de l'unité 1

```
interface ethernet1/8
```

```
no shutdown
description CCL

cluster group cluster1
local-unit asa1
cluster-interface ethernet1/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

Configuration de démarrage de l'unité de données de l'unité 2

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa2
cluster-interface ethernet1/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-data-node
```

Configuration de démarrage de l'unité de données de l'unité 3

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa3
cluster-interface ethernet1/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-data-node
```

Configuration de l'interface de l'unité de contrôle

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
no shutdown

interface ethernet1/1
channel-group 1 mode active
no shutdown

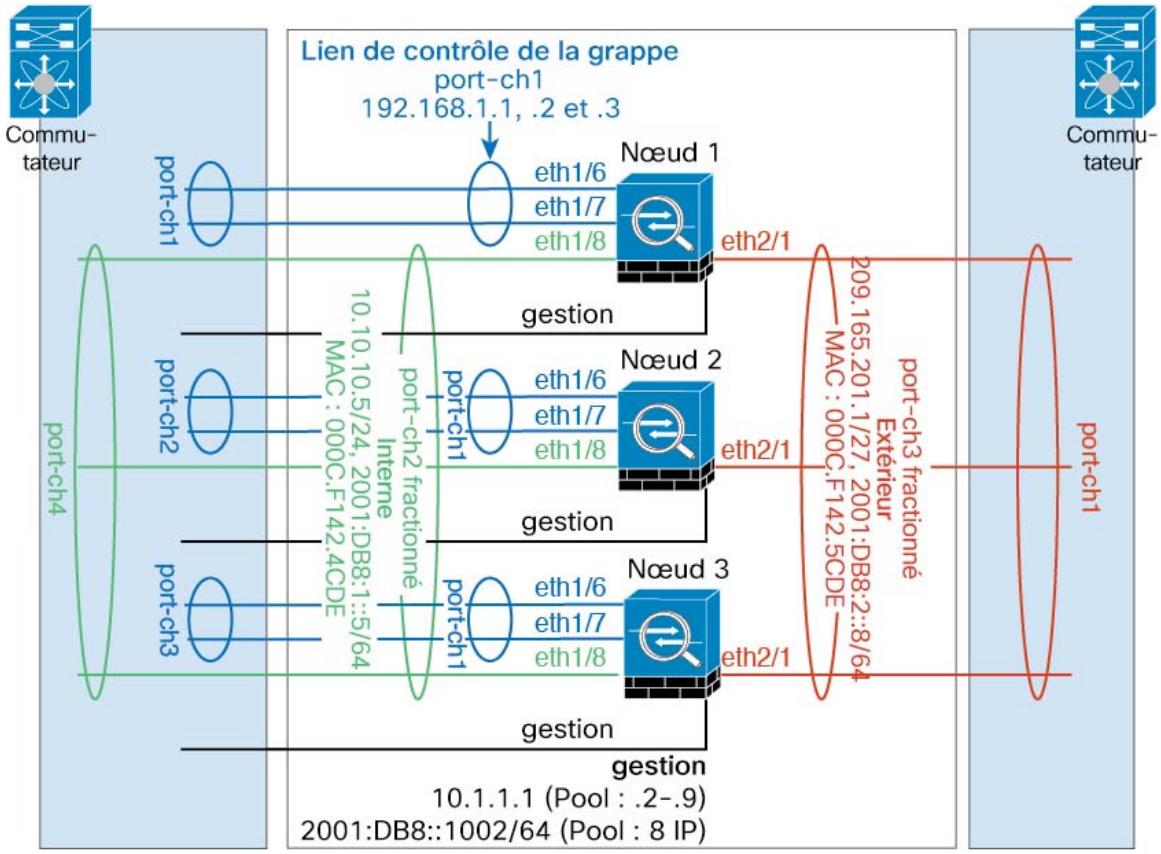
interface port-channel 1

interface port-channel 1.10
vlan 10
```

```
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface port-channel 1.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

Ségrégation du trafic



Vous pourriez souhaiter une séparation physique du trafic entre le réseau interne et le réseau externe.

Comme le montre le diagramme ci-dessus, il y a un EtherChannel étendu sur le côté gauche qui se connecte au commutateur interne et l'autre sur le côté droit au commutateur externe. Vous pouvez également créer des sous-interfaces VLAN sur chaque EtherChannel, au besoin.

Mode d'interface sur chaque unité

```
cluster interface-mode spanned force
```

Configuration de démarrage de l'unité de contrôle de l'unité 1

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa1
 cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
 priority 1
 key chuntheunavoidable
 enable noconfirm
```

Configuration de démarrage de l'unité de données de l'unité 2

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa2
 cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
 priority 2
 key chuntheunavoidable
 enable as-data-node
```

Configuration de démarrage de l'unité de données de l'unité 3

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa3
 cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
 priority 3
 key chuntheunavoidable
```

```
 enable as-data-node
```

Configuration de l'interface de l'unité de contrôle

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
 nameif management
 ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
 ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
 security-level 100
 management-only
 no shutdown

interface ethernet 1/8
 channel-group 2 mode active
 no shutdown

interface port-channel 2
 nameif inside
 ip address 10.10.10.5 255.255.255.0
 ipv6 address 2001:DB8:1::5/64
 mac-address 000C.F142.4CDE

interface ethernet 2/1
 channel-group 3 mode active
 no shutdown

interface port-channel 3
 nameif outside
 ip address 209.165.201.1 255.255.255.224
 ipv6 address 2001:DB8:2::8/64
 mac-address 000C.F142.5CDE
```

Configuration OTV pour la mise en grappe inter-sites en mode routé

La réussite de la mise en grappe inter-sites pour le mode routé avec les EtherChannels étendus dépend de la configuration et de la supervision appropriées de l'OTV. L'OTV joue un rôle majeur en transférant les paquets sur l'interface DCI. L'OTV transfère les paquets de monodiffusion sur l'interface DCI uniquement lorsqu'il apprend l'adresse MAC dans sa table de transfert. Si l'adresse MAC n'est pas apprise dans la table de transfert OTV, il abandonnera les paquets de monodiffusion.

Exemple de configuration OTV

```
//Sample OTV config:
//3151 – Inside VLAN, 3152 – Outside VLAN, 202 – CCL VLAN
//aaaa.1111.1234 – ASA inside interface global vMAC
//0050.56A8.3D22 – Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
```

```
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

Modifications du filtre OTV requises en raison d'une défaillance du site

Si un site tombe en panne, les filtres doivent être supprimés de l'OTV, car il n'est plus nécessaire de bloquer l'adresse MAC globale. Certaines configurations supplémentaires sont nécessaires.

Vous devez ajouter une entrée statique pour l'adresse MAC globale ASA sur le commutateur OTV dans le site qui est fonctionnel. Cette entrée permettra à l'OTV à l'autre extrémité d'ajouter ces entrées sur l'interface de superposition. Cette étape est nécessaire, car si le serveur et le client ont déjà l'entrée ARP pour l'ASA, ce qui est le cas pour les connexions existantes, ils n'enverront pas à nouveau l'ARP. Par conséquent, l'OTV n'aura pas la possibilité d'apprendre l'adresse MAC globale ASA dans sa table de transfert. Étant donné que l'OTV n'a pas l'adresse MAC globale dans sa table de transfert et que, conformément à sa conception, il ne diffusera pas de paquets de monodiffusion sur l'interface de superposition, il abandonnera les paquets de monodiffusion à l'adresse MAC globale du serveur, et les connexions existantes seront interrompues.

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

Lorsque l'autre site est restauré, vous devez ajouter de nouveau les filtres et supprimer cette entrée statique sur l'OTV. Il est très important d'effacer le tableau des adresses MAC dynamiques sur les deux OTV pour effacer l'entrée de superposition pour l'adresse MAC globale.

Effacement du tableau d'adresses MAC

Lorsqu'un site tombe en panne et qu'une entrée statique pour l'adresse MAC globale est ajoutée à l'OTV, vous devez laisser l'autre OTV apprendre l'adresse MAC globale sur l'interface de superposition. Une fois l'autre site rétabli, ces entrées doivent être effacées. Assurez-vous d'effacer la table d'adresses MAC pour vous assurer que l'OTV ne conserve aucune de ces entrées dans sa table de transfert.

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
```

```
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

Supervision du cache OTV ARP

Le service OTV gère un cache ARP pour mandataire ARP pour les adresses IP qu'il a apprises sur l'interface OTV.

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

Exemples de mise en grappe inter-sites

Les exemples suivants montrent les déploiements de grappe pris en charge.

Exemple de mode de routage EtherChannel étendu avec des adresses MAC et IP propres au site

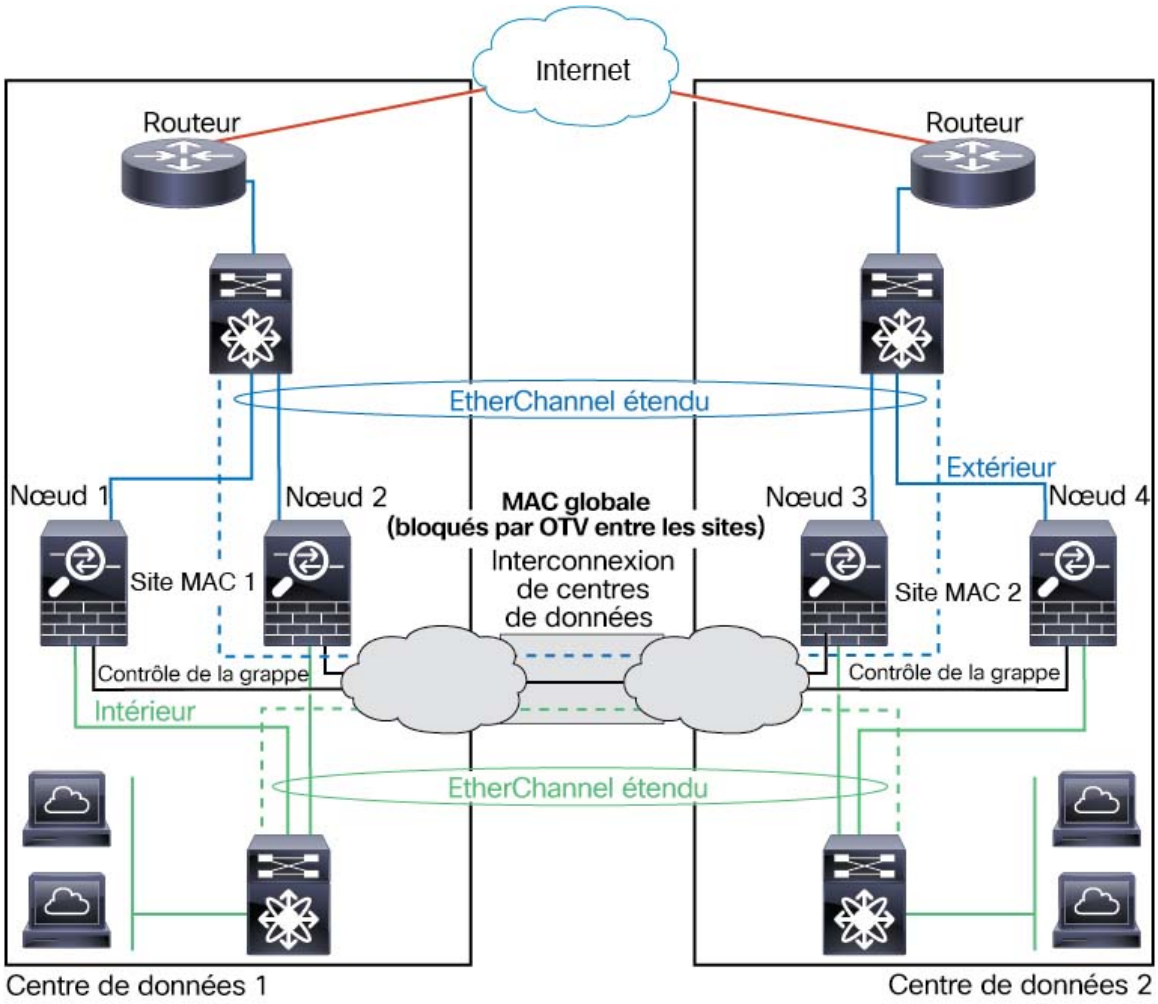
L'exemple suivant montre deux membres de la grappe dans chacun des deux centres de données, placés entre le routeur de passerelle et un réseau interne sur chaque site (insertion est-ouest). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux en utilisant des EtherChannels étendus pour le réseau interne et externe. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Les VLAN de données sont étendus entre les sites à l'aide de la virtualisation du transport par superposition (OTV) (ou d'un outil similaire). Vous devez ajouter des filtres bloquant l'adresse MAC globale pour empêcher le trafic de traverser l'interface DCI vers l'autre site lorsqu'il est destiné à la grappe. Si les nœuds de la grappe d'un site deviennent inaccessibles, vous devez supprimer les filtres pour que le trafic puisse être dirigé vers les nœuds de la grappe de l'autre site. Vous devez utiliser les adresses VACL pour filtrer l'adresse MAC globale.Pour certains commutateurs, comme le Nexus avec la carte de ligne de la gamme F3, vous devez également utiliser l'inspection ARP pour bloquer les paquets ARP de l'adresse MAC globale. L'inspection ARP nécessite que vous définissiez à la fois l'adresse MAC et l'adresse IP du site sur l'ASA. Si vous configurez uniquement l'adresse MAC du site N'oubliez pas de désactiver l'inspection ARP.

La grappe sert de passerelle pour les réseaux internes. Le MAC virtuel global, qui est partagé sur tous les nœuds de la grappe, est utilisé uniquement pour recevoir des paquets. Les paquets sortants utilisent une adresse MAC spécifique au site pour chaque grappe de contrôleurs de domaine. Cette fonctionnalité empêche les commutateurs d'apprendre la même adresse MAC globale à partir des deux sites sur deux ports différents, ce qui entraîne une oscillation MAC; au lieu de cela, ils connaissent uniquement l'adresse MAC du site.

Dans ce scénario :

- Tous les paquets de sortie envoyés par la grappe utilisent l'adresse MAC du site et sont localisés dans le centre de données.
- Tous les paquets entrants vers la grappe sont envoyés à l'aide de l'adresse MAC globale, de sorte qu'ils peuvent être reçus par n'importe quel nœud des deux sites; les filtres de l'OTV localisent le trafic dans le centre de données.



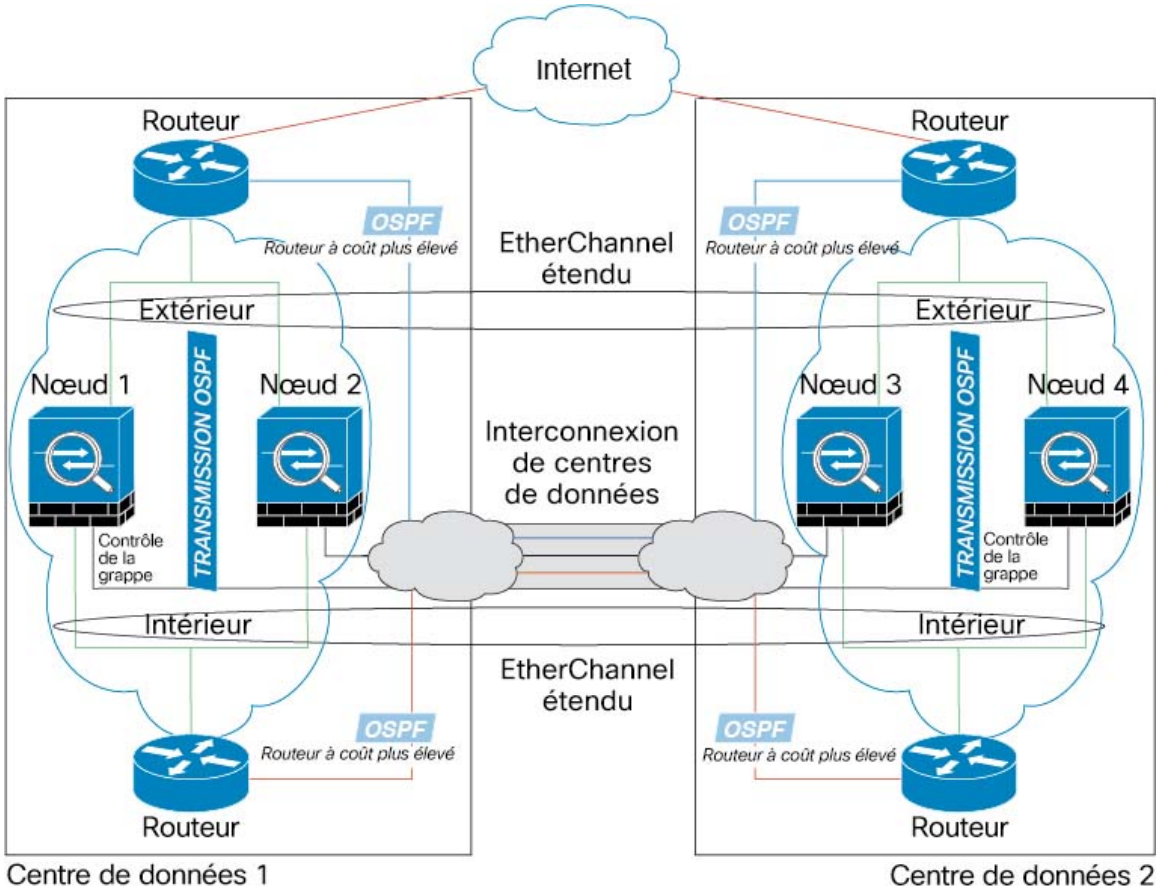
Exemple intersites nord-sud de mode transparent de l'EtherChannel étendu

L'exemple suivant montre 2 membres de la grappe dans chacun des 2 centres de données placés entre les routeurs internes et externes (insertion nord-sud). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux en utilisant des EtherChannels étendus pour l'intérieur et l'extérieur. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Les routeurs internes et externes de chaque centre de données utilisent le protocole OSPF, qui est transmis par les périphériques ASA transparents. Contrairement aux MAC, les adresses IP des routeurs sont uniques sur tous les routeurs. En attribuant un routage à coût plus élevé sur l'interface DCI, le trafic reste dans chaque centre de données, sauf si tous les membres de la grappe d'un site donné tombent en panne. La voie de routage la moins dispendieuse qui traverse les ASA doit traverser le même groupe de ponts sur chaque site pour que la grappe puisse maintenir des connexions dissymétriques. En cas de défaillance de tous les membres de la grappe sur un site, le trafic passe de chaque routeur sur l'interface DCI aux membres de la grappe sur l'autre site.

La mise en œuvre des commutateurs sur chaque site peut inclure :

- VSS inter-sites, vPC, StackWise ou StackWise Virtual : dans ce scénario, vous installez un commutateur au centre de données 1, et l'autre au centre de données 2. Une option consiste à ce que les nœuds de la grappe de chaque centre de données se connectent uniquement au commutateur local, tandis que le trafic du commutateur redondant traverse le DCI. Dans ce cas, les connexions sont pour la plupart conservées localement à chaque centre de données. Vous pouvez éventuellement connecter chaque nœud aux deux commutateurs de la DCI si la DCI peut gérer le trafic supplémentaire. Dans ce cas, le trafic est réparti entre les centres de données, il est donc essentiel que l'interface DCI soit très robuste.
- Local VSS, vPC, StackWise ou StackWise Virtual sur chaque site : Pour une meilleure redondance des commutateurs, vous pouvez installer 2 paires de commutateurs redondants distincts sur chaque site. Dans ce cas, bien que les nœuds de la grappe aient toujours un EtherChannel étendu avec le châssis du centre de données 1 connecté uniquement aux deux commutateurs locaux et le châssis du centre de données 2 connecté à ces commutateurs locaux, l'EtherChannel étendu est essentiellement « divisé ». Chaque système de commutation local redondant voit l'EtherChannel étendu comme un EtherChannel local au site.

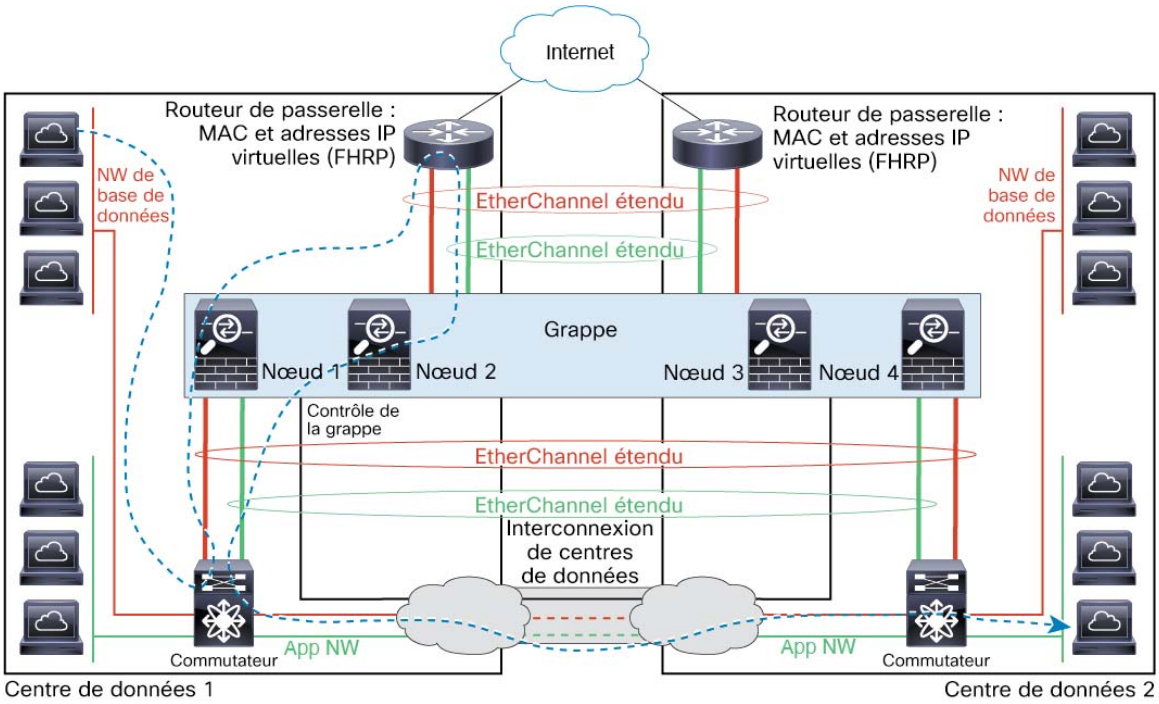


Exemple inter-sites est-ouest en mode transparent de l'EtherChannel étendu

L'exemple suivant montre deux membres de la grappe dans chacun des deux centres de données, placés entre le routeur de la passerelle et deux réseaux internes sur chaque site, le réseau d'applications et le réseau de base de données (insertion est-ouest). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux au

moyen d'EtherChannels étendus pour les réseaux App et DB à l'intérieur et à l'extérieur. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Le routeur de la passerelle de chaque site utilise un FHRP comme le HSRP pour fournir les mêmes adresses MAC virtuelles et IP de destination sur chaque site. Une bonne pratique pour éviter le basculement involontaire des adresses MAC consiste à ajouter de manière statique les adresses MAC réelles des routeurs de passerelle au tableau d'adresses MAC de l'ASA à l'aide de la commande **mac-address-table static** *outside_interface mac_address*. Sans ces entrées, si la passerelle du site 1 communique avec la passerelle du site 2, ce trafic pourrait passer par l'ASA et tenter d'atteindre le site 2 à partir de l'interface interne, ce qui poserait des problèmes. Les VLAN de données sont étendus entre les sites à l'aide de la virtualisation du transport par superposition (OTV) (ou d'un outil similaire). Vous devez ajouter des filtres pour empêcher le trafic de traverser l'interface DCI vers l'autre site lorsqu'il est destiné au routeur de la passerelle. Si le routeur de la passerelle d'un site devient inaccessible, vous devez supprimer les filtres pour que le trafic puisse être dirigé vers le routeur de la passerelle de l'autre site.



Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe de l'ASA

Certaines fonctionnalités d'ASA ne sont pas prises en charge avec la mise en grappe d'ASA, et d'autres le sont uniquement sur le nœud de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

- Fonctionnalités de communication unifiée qui reposent sur le mandataire TLS
- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Interfaces de tunnel virtuel (VTI)
- Les inspections d'application suivantes :
  - CTIQBE
  - H323, H225 et RAS
  - Intercommunication IPsec
  - MGCP
  - MMP
  - RTSP
  - SCCP (Skinny)
  - WAAS
  - WCCP
- Filtre de trafic de réseau de zombies
- Auto Update Server
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Équilibrage de la charge VPN
- Basculement
- Routage et pont intégrés
- Mode FIPS

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.

Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET
  - SunRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique
- Autorisation et authentification pour l'accès réseau La comptabilité est décentralisée.
- Services de filtrage
- VPN de site à site
- Traitement du protocole du plan de contrôle de multidiffusion IGMP (le transfert du plan de données est distribué dans la grappe)
- Traitement du protocole du plan de contrôle de multidiffusion PIM (le transfert du plan de données est distribué dans la grappe)
- Routage dynamique

Fonctionnalités appliquées aux nœuds individuels

Ces fonctionnalités sont appliquées à chaque nœud ASA, plutôt qu'à la grappe dans son ensemble ou au nœud de contrôle.

- QoS : la politique QoS est synchronisée dans la grappe dans le cadre de la duplication de la configuration. Cependant, la politique est appliquée sur chaque nœud indépendamment. Par exemple, si vous configurez le contrôle en sortie, les valeurs de débit de conformité et de rafale de conformité s'appliquent au trafic sortant d'un ASA particulier. Dans une grappe à 3 nœuds et avec le trafic réparti uniformément, le taux de conformité devient en fait trois fois supérieur au débit de la grappe.
- Détection des menaces : la détection des menaces fonctionne sur chaque nœud indépendamment; par exemple, les statistiques principales sont propres au nœud. La détection de l'analyse de port, par exemple, ne fonctionne pas, car l'analyse du trafic sera équilibrée entre tous les nœuds et un nœud ne verra pas tout le trafic.
- Gestion des ressources : la gestion des ressources en mode contexte multiple est appliquée séparément sur chaque nœud en fonction de l'utilisation locale.
- Trafic LISP : le trafic LISP sur le port UDP 4342 est inspecté par chaque nœud de réception, mais aucun directeur n'est affecté. Chaque nœud ajoute au tableau EID qui est partagé dans la grappe, mais le trafic LISP lui-même ne participe pas au partage de l'état de la grappe.

AAA pour l'accès réseau et la mise en grappe

L'AAA pour l'accès réseau comprend trois composants : l'authentification, l'autorisation et la gestion de comptes. L'authentification et l'autorisation sont mises en œuvre en tant que fonctionnalités centralisées sur le nœud de contrôle de mise en grappe avec la duplication des structures de données sur les nœuds de données de grappe. Si un nœud de contrôle est choisi, le nouveau nœud de contrôle disposera de toute l'information nécessaire pour continuer le fonctionnement ininterrompu des utilisateurs authentifiés établis et de leurs autorisations associées. Les délais d'inactivité et absolue pour l'authentification des utilisateurs sont conservés lors d'un changement de nœud de contrôle se produit.

La comptabilité est mise en œuvre en tant que fonctionnalité distribuée dans une grappe. La comptabilité est effectuée flux par flux, de sorte que le nœud de la grappe possédant un flux enverra les messages de démarrage et d'arrêt de comptabilité au serveur AAA lorsque la comptabilité est configurée pour un flux.

Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe (voir les commandes **set connection conn-max**, **set connection embryonic-conn-max**, **set connection per-client-embryonic-max**, et **set connection per-client-max**). Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.
- Si vous utilisez l'AAA pour l'accès FTP, le flux du canal de contrôle est centralisé sur le nœud de contrôle.

Inspection ICMP et mise en grappe

Le flux des paquets d'erreurs ICMP et ICMP dans la grappe varie selon que l'inspection d'erreurs ICMP ou ICMP est activée ou non. Sans inspection ICMP, ICMP est un flux unidirectionnel et il n'y a pas de prise en charge de flux directeur. Avec l'inspection ICMP, le flux ICMP devient bidirectionnel et est soutenu par un flux directeur/de sauvegarde. L'une des différences avec un flux ICMP inspecté réside dans le traitement par le directeur du paquet transféré : le directeur transmettra le paquet de réponse d'écho ICMP au propriétaire du flux au lieu de retourner le paquet au transitaire.

Routage multidiffusion et mise en grappe

Routage multidiffusion en mode EtherChannel étendu

En mode EtherChannel étendu : l'unité de contrôle gère tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi. Une fois la connexion établie, chaque unité de données peut transférer des paquets de données en multidiffusion.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents ASAdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à ASA qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.

- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, la grappe divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.
- Réutiliser un pool PAT dans plusieurs règles : pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.
- Fonctionnalité PAT par session : bien qu'elle ne soit pas exclusive à la mise en grappe, la fonctionnalité PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque nœud de données de posséder des connexions PAT; en revanche, les connexions PAT multisessions doivent être transférées au nœud de contrôle et détenues par celui-ci. Par défaut, tout le trafic TCP et le trafic DNS UDP utilisent un xlate PAT par session, tandis que ICMP et tout le reste du trafic UDP utilise la multisession. Vous pouvez configurer des règles NAT par session pour modifier ces valeurs par défaut pour TCP et UDP, mais vous ne pouvez pas configurer la PAT par session pour ICMP. Par exemple, en raison de l'utilisation croissante du protocole Quic sur le port UDP/443 comme alternative de performance à HTTPS TLS sur TCP/443, vous devriez activer la traduction d'adresses par session (PAT) pour UDP/443. Pour le trafic qui bénéficie de la PAT multisession, comme le H.323, le SIP ou l'interface simplifiée, vous pouvez désactiver la PAT par session pour les ports TCP associés (les ports UDP de ces ports H.323 et SIP sont déjà multisession en par défaut). Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.
- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP

- XDMCP
- SIP

- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

Routage et mise en grappe dynamiques

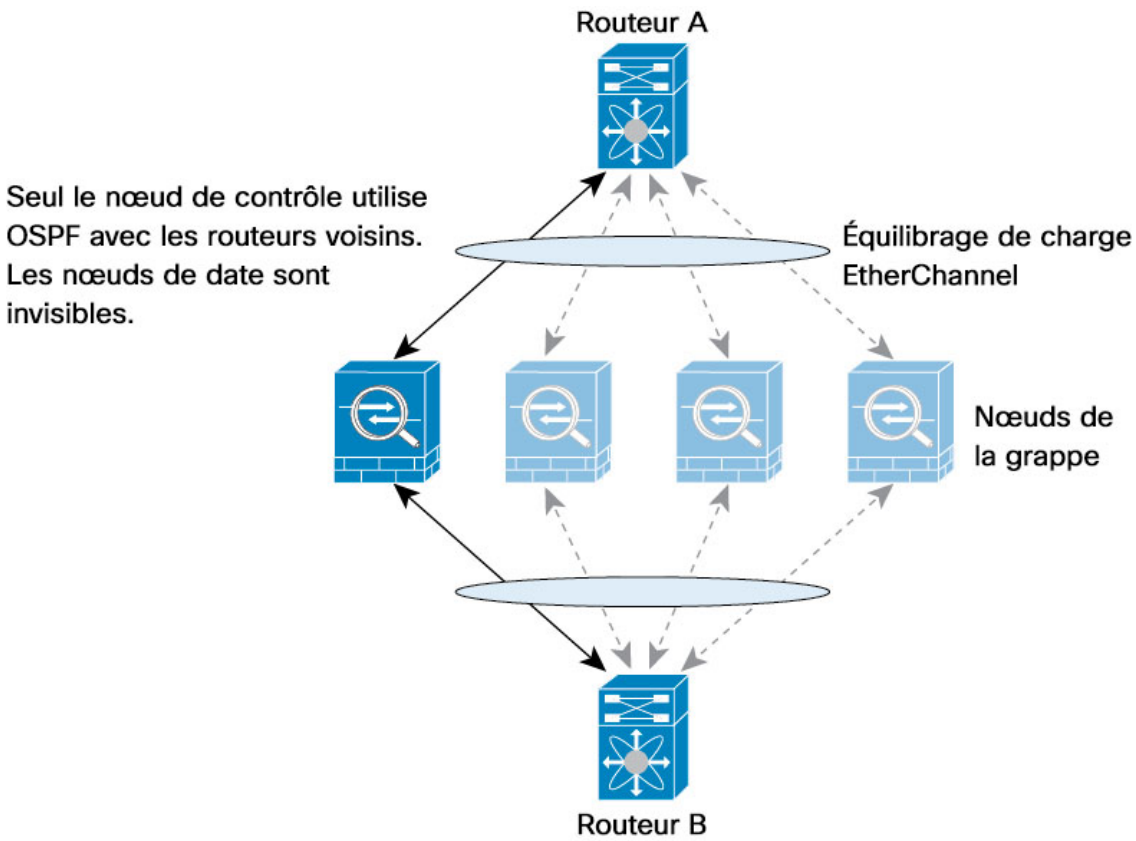
Cette section décrit comment utiliser le routage dynamique avec la mise en grappe.

Routage dynamique en mode EtherChannel étendu

Remarque IS-IS n'est pas pris en charge en mode EtherChannel étendu.

Le processus de routage ne s'exécute que sur le nœud de contrôle, et les routes sont apprises par le nœud de contrôle et répliquées sur les nœuds de données. Si un paquet de routage arrive à un nœud de données, il est redirigé vers le nœud de contrôle.

Illustration 50 : Routage dynamique en mode EtherChannel étendu



Une fois que le nœud de données a appris les routes du nœud de contrôle, chaque nœud prend des décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée du nœud de contrôle avec les nœuds de données. S'il y a basculement du nœud de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

SCTP et mise en grappe

Une association SCTP peut être créée sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses connexions multi-hébergement doivent résider sur le même nœud.

Inspection SIP et mise en grappe

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

La configuration du mandataire TLS n'est pas prise en charge.

SNMP et mise en grappe

Un agent SNMP interroge chaque ASA en fonction de l'adresse IP locale de son . Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud.Vous devez les rajouter sur le nœud de contrôle pour forcer les utilisateurs à se reproduire vers le nouveau nœud, ou directement sur le nœud de données.

STUN et mise en grappe

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Syslog, NetFlow et la mise en grappe

- Syslog : chaque nœud de la grappe génère ses propres messages de journal système. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.

- NetFlow : chaque nœud de la grappe génère son propre flux NetFlow. Le collecteur NetFlow peut traiter chaque appareil ASA uniquement comme un exportateur NetFlow distinct.

Cisco TrustSec et la mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; seul le nœud de contrôle prend en charge les connexions VPN.



Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Lorsque vous connectez un tunnel VPN à une adresse EtherChannel étendu, les connexions sont automatiquement transférées au nœud de contrôle.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

Choix du nœud de contrôle

Les nœuds de la grappe communiquent sur la liaison de commande de grappe pour élire un nœud de contrôle comme suit :

1. Lorsque vous activez la mise en grappe pour un nœud (ou lorsqu'il démarre avec la mise en grappe déjà activée), il diffuse une demande de sélection toutes les 3 secondes.
2. Tous les autres nœuds ayant une priorité plus élevée répondent à la demande de sélection; la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.

Remarque Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud se joint ultérieurement à la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle; le nœud de contrôle existant demeure toujours le nœud de contrôle, sauf s'il s'arrête de répondre, moment auquel un nouveau nœud de contrôle est sélectionné.
5. Dans un scénario de « discernement partagé », où il y a temporairement plusieurs nœuds de contrôle, le nœud ayant la priorité la plus élevée conserve le rôle tandis que les autres nœuds retournent aux rôles de nœud de données.

Remarque Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

Surveillance de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Consultez Choix du nœud de contrôle, à la page 436 pour de plus amples renseignements.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

- Spanned EtherChannel (EtherChannel étendu) : Utilise le protocole cLACP (cluster Link Aggregation Control Protocol). Chaque nœud surveille l'état de la liaison et les messages du protocole cLACP pour déterminer si le port est toujours actif dans l'EtherChannel. L'état est signalé au nœud de contrôle.

Lorsque vous activez la surveillance de l'intégrité, toutes les interfaces physiques (y compris les interfaces EtherChannel principales) sont surveillées par défaut; vous pouvez éventuellement désactiver la surveillance par interface. Seules les interfaces nommées peuvent être surveillées. Par exemple, l'EtherChannel désigné doit échouer pour être considéré comme en échec, ce qui signifie que tous les ports membres d'un EtherChannel ne doivent pas déclencher la suppression de la grappe (selon le paramètre minimal de groupement de ports).

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le délai avant que ASA ne supprime un membre de la grappe dépend dépend du fait que le nœud est un membre établi ou en train de se joindre à la grappe. si l'interface est en panne sur un membre établi, le ASA supprime le membre après 9 secondes. L'ASA ne surveille pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de ASA de la grappe. Pour les non-EtherChannels, le nœud est supprimé après 500 ms, quel que soit l'état membre.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

ASA tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.



Remarque Lorsque ASA devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Rejoindre la grappe

Après le retrait d'un nœud de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe au niveau du port de console en saisissant la commande **cluster group** *name*, puis **enable**.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : l'ASA essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment. Ce comportement est configurable.
- Échec de l'interface de données : l'ASA tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'ASA désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe au niveau du port de console en saisissant la commande **cluster group** *name*, puis **enable**. Ce comportement est configurable.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que la liaison

de commande de grappe soit active et que la mise en grappe soit toujours activée avec la commande **enable**. L'ASA tente de rejoindre la grappe toutes les 5 secondes.

- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc. Un nœud tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Ce comportement est configurable.

Consultez Configurer les paramètres de démarrage du nœud de contrôle, à la page 378.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 18 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
Tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	Comprend les règles AAA (uauth).
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—
VPN distribué (site à site) pour Firepower 4100/9300	Oui	La session de sauvegarde devient la session active, puis une nouvelle session de sauvegarde est créée.

Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue,

lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.

- Propriétaire du sauvegarde : nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis.

  Si vous activez la localisation du directeur pour la mise en grappe inter-sites, il existe deux rôles de propriétaire de la sauvegarde : le rôle de sauvegarde locale et de sauvegarde globale. Le propriétaire choisit toujours une sauvegarde locale sur le même site que lui (en fonction de l'ID du site). La sauvegarde globale peut se trouver sur n'importe quel site et peut même se trouver sur le même nœud que la sauvegarde locale. Le propriétaire envoie des informations sur l'état de la connexion aux deux sauvegardes.

  Si vous activez la redondance de sites et que le propriétaire de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La sauvegarde de châssis et la sauvegarde de site sont indépendantes. Par conséquent, dans certains cas, un flux comportera à la fois une sauvegarde de châssis et une sauvegarde de site.

- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Si vous activez la localisation de directeur pour la mise en grappe inter-sites, il y a deux rôles de directeur : le directeur local et le directeur global. Le propriétaire choisit toujours un directeur local sur le même site que lui (en fonction de l'ID du site). Le directeur global peut être sur n'importe quel site et peut même être le même nœud que le directeur local. En cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site.

  Détails du hachage ICMP/ICMPv6 :

  - Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
  - Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
  - Pour les autres paquets, les ports source et de destination sont à 0.

- Transitaire : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Si vous activez la localisation de directeur, le redirecteur interroge toujours le directeur local. Le transitaire n'interroge le directeur global que si le directeur local ne connaît pas le propriétaire, par exemple, si un membre de la grappe reçoit des paquets pour une connexion qui appartient à un autre site. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.



Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- Propriétaire de fragment : pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Connexions par traduction d'adresse de port

Lorsqu'une connexion utilise la traduction d'adresses de port (PAT), le type de PAT (par session ou multisession) influence quel membre de la grappe devient propriétaire de la nouvelle connexion :

- PAT par session : le propriétaire est le nœud qui reçoit le paquet initial dans la connexion.

  Par défaut, le trafic TCP et DNS UDP utilise une PAT par session.

- PAT multisession : le propriétaire est toujours le nœud de contrôle. Si une connexion PAT multisession est initialement reçue par un nœud de données, le nœud de données transfère la connexion au nœud de contrôle.

  Par défaut, le trafic UDP (à l'exception du trafic UDP DNS) et ICMP utilise la PAT multisession. Ces connexions appartiennent donc toujours au nœud de contrôle.

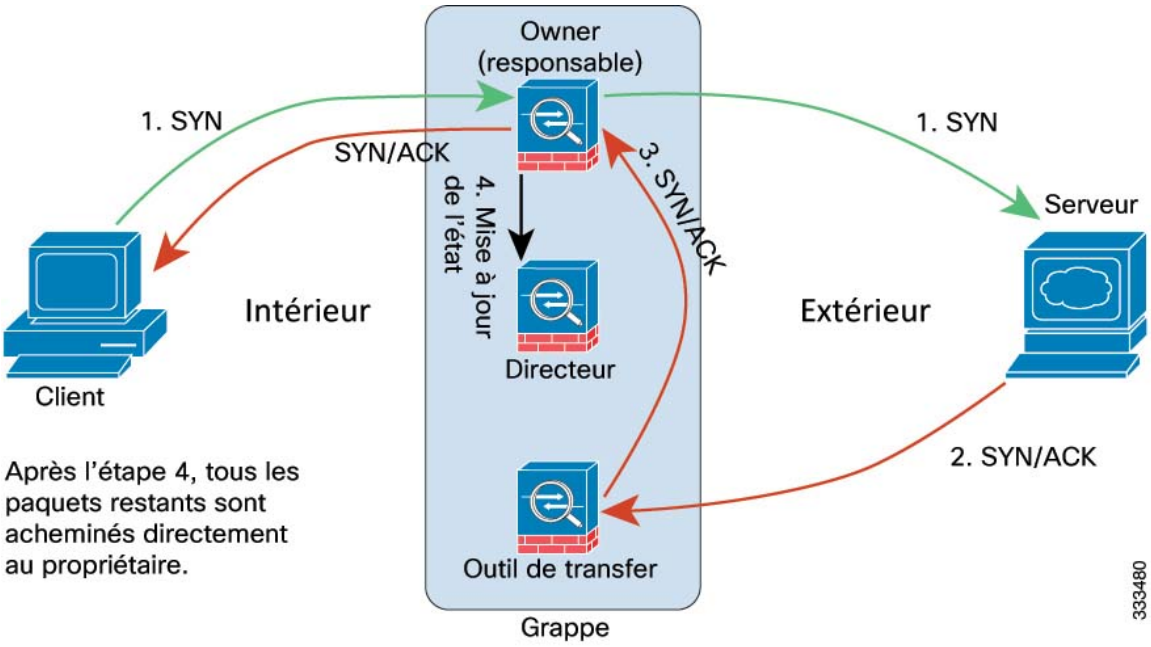
Vous pouvez modifier les valeurs par défaut de PAT par session pour les protocoles TCP et UDP afin que les connexions à ces protocoles soient gérées par session ou multisession selon la configuration. Pour ICMP, vous ne pouvez pas modifier la PAT multisession par défaut. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Pour de meilleures performances, un bon équilibrage de la charge externe est nécessaire pour que les deux directions d'un flux arrivent au même nœud et pour que les flux soient répartis uniformément entre les nœuds. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.



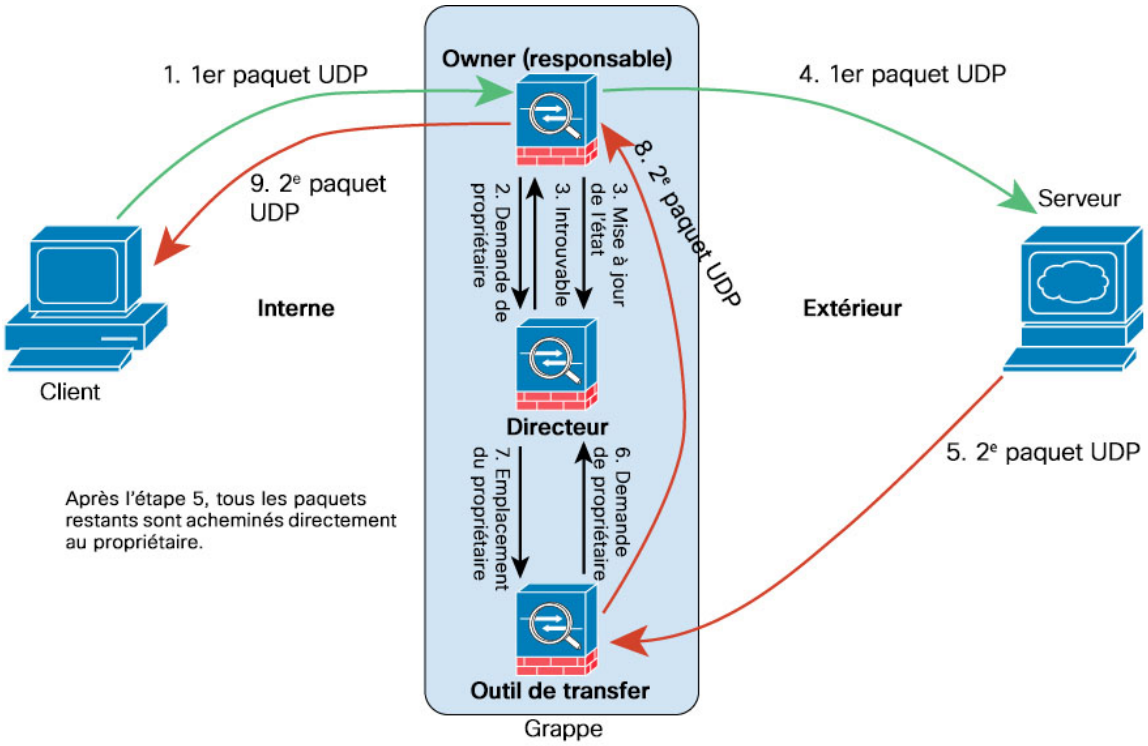
1. Le paquet SYN provient du client et est livré à un ASA (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un ASA différent (selon la méthode d'équilibrage de la charge). Cet ASA est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.
5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.

7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. ***Illustration 51 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un ASA (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.
6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.

8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Rééquilibrage des nouvelles connexions TCP dans la grappe

Si les capacités d'équilibrage de charges des routeurs en amont ou en aval entraînent une répartition non équilibrée des flux, vous pouvez configurer un rééquilibrage des nouvelles connexions afin que les nœuds ayant le plus de nouvelles connexions par seconde redirigent les nouveaux flux TCP vers d'autres nœuds. Aucun flux existant ne sera déplacé vers d'autres nœuds.

Comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Historique de la mise en grappe d'ASA pour le Secure Firewall

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
VPN site à site distribué avec mise en grappe sur le modèle Cisco Secure Firewall 4200	9.23(1)	Une grappe ASA sur le modèle Cisco Secure Firewall 4200 prend en charge le VPN de site à site en mode distribué. Le mode distribué permet d'avoir de nombreuses connexions VPN IPsec IKEv2 de site à site réparties sur les membres d'une grappe ASA, pas seulement sur le nœud de contrôle (comme en mode centralisé). Cela étend considérablement la prise en charge des VPN au-delà des capacités VPN centralisées et offre une haute disponibilité. Commandes ajoutées ou modifiées : **cluster redistribute vpn-sessiondb**, **show cluster vpn-sessiondb**, **vpn-mode**, **show cluster resource usage**, **show vpn-sessiondb** , **show conn detail**, **show crypto ikev2 stats**
Suppression des propos tendancieux	9.19(1)	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
La prise en charge de la mise en grappe sur le pare-feu Secure Firewall 3100 a été introduite	9.17(1)	Vous pouvez mettre en grappe jusqu'à 8 nœuds Secure Firewall 3100 en mode EtherChannel étendu.



CHAPITRE 11

Grappe ASA pour le Firepower 4100/9300

La mise en grappe vous permet de regrouper plusieurs Châssis Firepower 4100/9300 en un seul périphérique logique. La série Châssis Firepower 4100/9300 comprend les Firepower 9300 et Firepower 4100. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 522.

- À propos de la mise en grappe sur les châssis Firepower 4100/9300, à la page 445
- Exigences et conditions préalables à la mise en grappe sur Châssis Firepower 4100/9300 , à la page 452
- Licences pour la mise en grappe sur le Châssis Firepower 4100/9300 , à la page 454
- Lignes directrices et limites de la mise en grappe, à la page 455
- Configurer la mise en grappe sur le Châssis Firepower 4100/9300 , à la page 460
- FXOS : supprimer un nœud de la grappe, à la page 495
- ASA : Gérer les membres de la grappe, à la page 497
- ASA : supervision de la grappe ASA sur le Châssis Firepower 4100/9300 , à la page 501
- Dépannage du VPN S2S distribué, à la page 512
- Exemples de mise en grappe d'ASA, à la page 514
- Référence pour la mise en grappe, à la page 522
- Historique de la mise en grappe d'ASA sur le Firepower 4100/9300, à la page 538

À propos de la mise en grappe sur les châssis Firepower 4100/9300

Lorsque vous déployez une grappe sur le Châssis Firepower 4100/9300 , elle effectue les opérations suivantes :

- crée une *liaison de commande de grappe* (par défaut, le canal de port 48) pour la communication de nœud à nœud.

  Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, ce lien utilise le fond de panier Firepower 9300 pour les communications de la grappe.

Pour la mise en grappe avec plusieurs châssis, vous devez affecter manuellement une ou plusieurs interfaces physiques à cet EtherChannel pour les communications entre les châssis.

- Crée la configuration de démarrage de grappe dans l'application.

  Lorsque vous déployez la grappe, le superviseur de châssis envoie une configuration de démarrage minimale à chaque unité, qui comprend le nom de la grappe, l'interface de liaison de commande de grappe et d'autres paramètres de la grappe. Certaines parties de la configuration de démarrage peuvent être configurées par l'utilisateur dans l'application si vous souhaitez personnaliser votre environnement de mise en grappe.

- Affecte des interfaces de données à la grappe en tant *qu'interfaces étendues*.

  Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, les interfaces étendues ne se limitent pas aux EtherChannels, comme c'est le cas pour la mise en grappe avec plusieurs châssis. Le superviseur Firepower 9300 utilise la technologie EtherChannel en interne pour équilibrer la charge du trafic vers plusieurs modules sur une interface partagée, de sorte que tout type d'interface de données fonctionne pour le mode étendu. Pour la mise en grappe avec plusieurs châssis, vous devez utiliser des EtherChannels étendus pour toutes les interfaces de données.

Remarque Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

- Attribue une interface de gestion à toutes les unités de la grappe.

Voir l'une des sections suivantes pour plus d'informations sur la mise en grappe.

Configuration du démarrage

Lorsque vous déployez la grappe, le superviseur de châssis Firepower 4100/9300 envoie une configuration de démarrage minimale à chaque unité, qui comprend le nom de la grappe, l'interface de liaison de commande de grappe et d'autres paramètres de la grappe. Certaines parties de la configuration de démarrage sont configurables par l'utilisateur si vous souhaitez personnaliser votre environnement de mise en grappe.

Membres de la grappe

Les membres de la grappe collaborent pour partager la politique de sécurité et les flux de trafic.

L'unité de **contrôle** est l'un des membres de la grappe. L'unité de contrôle est déterminée automatiquement. Tous les autres membres sont des unités de **données**.

Vous devez effectuer toute la configuration sur l'unité de contrôle uniquement; la configuration est ensuite reproduite dans les unités de données.

Certaines fonctionnalités ne sont pas évolutives dans une grappe, et l'unité de contrôle gère tout le trafic pour ces fonctionnalités. Voir Fonctionnalités centralisées pour la mise en grappe, à la page 523.

Liaison de commande de grappe

La liaison de commande de grappe est un EtherChannel (canal de port 48) pour la communication d'unité à unité. Pour la mise en grappe intra-châssis, cette liaison utilise le fond de panier Firepower 9300 pour les

communications de la grappe. Pour la mise en grappe inter-châssis, vous devez affecter manuellement une ou plusieurs interfaces physiques à cet EtherChannel sur le Châssis Firepower 4100/9300 pour les communications entre les châssis.

Dans le cas d'une grappe inter-châssis à deux châssis, ne connectez pas directement la liaison de commande de grappe d'un châssis à l'autre. Si vous connectez directement les interfaces, lorsqu'une unité tombe en panne, la liaison de commande de grappe tombe en panne, et donc l'unité intègre restante. Si vous connectez la liaison de commande de grappe par l'intermédiaire d'un commutateur, cette dernière reste active pour l'unité intègre.

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Consultez les sections suivantes pour en savoir plus sur la liaison de commande de grappe.

Dimensionner la liaison de commande de grappe

Si possible, vous devez dimensionner la liaison de commande de grappe en fonction du débit attendu de chaque châssis afin que la liaison de commande de grappe puisse gérer les scénarios les plus défavorables.

Le trafic de liaison de commande de grappe est principalement composé de mises à jour d'état et de paquets transférés. Le volume de trafic varie à un moment donné sur la liaison de commande de grappe. La quantité de trafic transféré dépend de l'efficacité de l'équilibrage de la charge et de l'importance du trafic pour les fonctionnalités centralisées. Par exemple :

- La NAT entraîne un mauvais équilibrage de la charge des connexions et la nécessité de rééquilibrer tout le trafic de retour vers les bonnes unités.
- L'AAA pour l'accès réseau est une fonctionnalité centralisée, de sorte que tout le trafic est acheminé à l'unité de contrôle.
- Lorsque les membres changent, la grappe doit rééquilibrer un grand nombre de connexions, utilisant ainsi temporairement une grande quantité de bande passante de la liaison de commande de grappe.

Une liaison de commande de grappe à bande passante plus élevée aide la grappe à converger plus rapidement lorsque les membres changent et empêche les goulots d'étranglement.

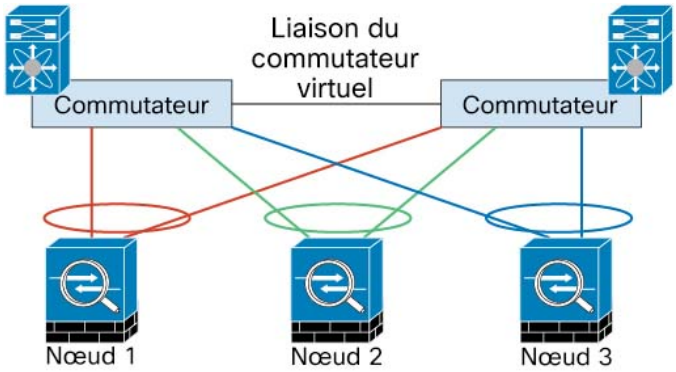


Remarque Si votre grappe génère un trafic asymétrique (rééquilibreur) important, vous devez augmenter la taille du lien de commande de grappe.

Redondance de la liaison de commande de la grappe

Nous vous recommandons d'utiliser un EtherChannel pour la liaison de commande de la grappe, afin de pouvoir transférer le trafic sur plusieurs liaisons de l'EtherChannel tout en assurant la redondance.

Le diagramme suivant montre comment utiliser un EtherChannel comme liaison de commande de la grappe dans un système de commutation virtuelle (VSS), un canal de port virtuel (vPC), un StackWise ou un environnement StackWise Virtual. Tous les liens de l'EtherChannel sont actifs. Lorsque le commutateur fait partie d'un système redondant, vous pouvez connecter des interfaces de pare-feu dans le même EtherChannel pour séparer les commutateurs du système redondant. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur. Notez qu'il s'agit d'un EtherChannel local au périphérique et non d'un EtherChannel étendu.



Fiabilité de la liaison de commande de grappe pour la mise en grappe

Pour assurer la fonctionnalité de la liaison de commande de grappe, vérifiez que le temps aller-retour (RTT) entre les unités est inférieur à 20 ms. Cette latence maximale améliore la compatibilité avec les membres de la grappe installés à différents sites géographiques. Pour vérifier votre latence, envoyez un message Ping sur la liaison de commande de grappe entre les unités.

La liaison de commande de grappe doit être fiable, sans paquets en désordre ou abandonnés; par exemple, pour un déploiement intersite, vous devez utiliser un lien dédié.

Réseau de liaison de commande de grappe

Le Châssis Firepower 4100/9300 génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID de châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot-id*.Vous pouvez personnaliser cette adresse IP lorsque vous déployez la grappe. Le réseau de liaison de commande de grappe ne peut pas comprendre de routeurs entre les unités; seule la commutation de couche 2 est autorisée. Pour le trafic intersites, Cisco recommande d'utiliser la virtualisation du transport par superposition (OTV).

Interfaces de la grappe

Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, vous pouvez affecter des interfaces physiques ou des EtherChannels (également appelés canaux de port) à la grappe. Les interfaces affectées à la grappe sont des interfaces étendues qui équilibrent la charge du trafic entre tous les membres de la grappe.

Pour la mise en grappe avec plusieurs châssis, vous pouvez uniquement affecter des EtherChannels de données à la grappe. Ces EtherChannels étendus comprennent les mêmes interfaces membre sur chaque châssis; Sur le commutateur en amont, toutes ces interfaces sont incluses dans un seul EtherChannel, de sorte que le commutateur ne sache pas qu'il est connecté à plusieurs périphériques.

Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

Connexion à un système de commutateurs redondants

Nous vous recommandons de connecter les EtherChannels à un système de commutation redondant tel qu'un VSS, vPC, StackWise ou un système virtuel StackWise pour assurer la redondance de vos interfaces.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

Gestion des grappes Cisco Secure Firewall ASA

L'un des avantages de l'utilisation de la mise en grappe ASA est la facilité de gestion. Cette section décrit comment gérer la grappe.

Réseau de gestion

Nous vous recommandons de connecter toutes les unités à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Interface de gestion

Vous devez affecter une interface de type gestion à la grappe. Cette interface est une interface individuelle spéciale, par opposition à une interface étendue. L'interface de gestion vous permet de vous connecter directement à chaque unité.

L'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours à l'unité de contrôle actuelle. Vous configurez également une plage d'adresses de sorte que chaque unité, y compris l'unité de contrôle actuelle, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de gestion cohérent à une adresse; lorsqu'une unité de contrôle change, l'adresse IP de la grappe principale est déplacée vers la nouvelle unité de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente.

Par exemple, vous pouvez gérer la grappe en vous connectant à l'adresse IP de la grappe principale, qui est toujours associée à l'unité de contrôle actuelle. Pour gérer un membre, vous pouvez vous connecter à l'adresse IP locale.



Remarque Le trafic vers la boîte doit être acheminé vers l'adresse IP de gestion du nœud; le trafic vers la boîte n'est pas transféré sur la liaison de commande de grappe vers un autre nœud.

Pour le trafic de gestion sortant tel que TFTP ou syslog, chaque unité, y compris l'unité de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Gestion de l'unité de contrôle vs Gestion de l'unité de données

Toutes la gestion et la surveillance peuvent avoir lieu sur le nœud de contrôle. À partir du nœud de contrôle, vous pouvez vérifier les statistiques d'exécution, l'utilisation des ressources ou d'autres informations de surveillance sur tous les nœuds. Vous pouvez également transmettre une commande à tous les nœuds de la grappe et reproduire les messages de console des nœuds de données vers le nœud de contrôle.

Vous pouvez surveiller directement les nœuds de données si vous le souhaitez. Bien que cela soit également disponible à partir du nœud de contrôle, vous pouvez effectuer la gestion de fichiers sur les nœuds de données (y compris la sauvegarde de la configuration et la mise à jour des images). Les fonctions suivantes ne sont pas disponibles à partir du nœud de commande :

- Surveillance des statistiques propres à la grappe par nœud.
- Surveillance des journaux système par nœud (sauf pour les journaux système envoyés à la console lorsque la duplication de la console est activée).
- SNMP
- NetFlow

duplication de clé de chiffrement

Lorsque vous créez une clé de chiffrement sur le nœud de contrôle, la clé est répliquée sur tous les nœuds de données. Si vous avez une session SSH sur l'adresse IP de la grappe principale, vous serez déconnecté en cas de défaillance du nœud de contrôle. Le nouveau nœud de contrôle utilise la même clé pour les connexions SSH, de sorte que vous n'avez pas besoin de mettre à jour la clé d'hôte SSH mise en cache lorsque vous vous reconnectez au nouveau nœud de contrôle.

Incompatibilité d'adresse IP du certificat de connexion ASDM

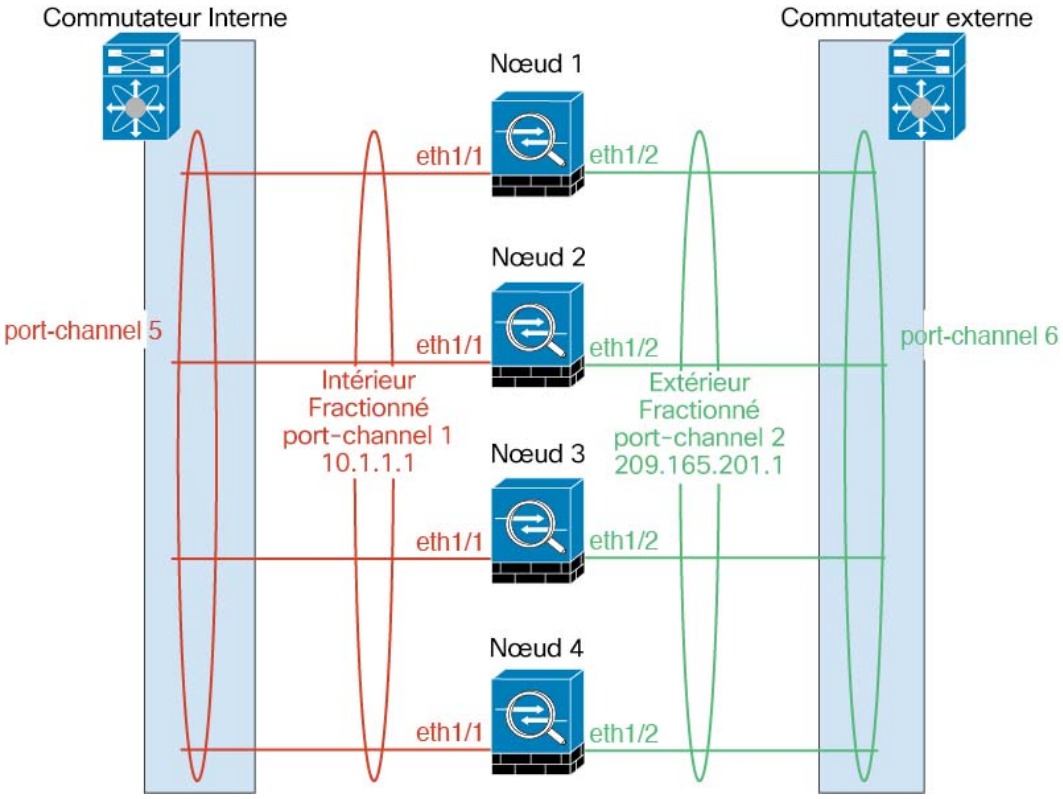
Par défaut, un certificat autosigné est utilisé pour la connexion ASDM en fonction de l'adresse IP locale. Si vous vous connectez à l'adresse IP de la grappe principale à l'aide d'ASDM, un message d'avertissement concernant une adresse IP non concordante peut s'afficher, car le certificat utilise l'adresse IP locale, et non l'adresse IP de la grappe principale. Vous pouvez ignorer le message et établir la connexion ASDM. Cependant, pour éviter ce type d'avertissement, vous pouvez inscrire un certificat qui contient l'adresse IP de la grappe principale et toutes les adresses IP locales de l'ensemble d'adresses IP. Vous pouvez ensuite utiliser ce certificat pour chaque membre de la grappe. Consultez https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html pour de plus amples renseignements.

EtherChannels étendus (recommandé)

Vous pouvez regrouper une ou plusieurs interfaces par châssis dans un EtherChannel qui s'étend sur tous les châssis de la grappe. L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal.

Un EtherChannel étendu peut être configuré dans les modes de pare-feu avec routage et transparent. En mode routé, l'EtherChannel est configuré comme une interface routée avec une seule adresse IP. En mode transparent, l'adresse IP est attribuée aux BVI, et non à l'interface du membre du groupe de ponts.

L'EtherChannel assure intrinsèquement l'équilibrage de la charge dans le cadre du fonctionnement de base.



Mise en grappe inter-sites

Pour les installations inter-sites, vous pouvez profiter de la mise en grappe d'ASA tant que vous suivez les lignes directrices recommandées.

Vous pouvez configurer chaque châssis de grappe pour qu'il appartienne à un ID de site distinct.

Les ID de site fonctionnent avec des adresses MAC et des adresses IPspécifiques au site . Les paquets qui sortent de la grappe utilisent une adresse MAC et une adresse IPpropres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IPglobales. Cette fonctionnalité empêche les commutateurs d'apprendre la même adresse MAC globale à partir des deux sites sur deux ports différents, ce qui entraîne une oscillation MAC; au lieu de cela, ils connaissent uniquement l'adresse MAC du site. Les adresses MAC et les adresses IP spécifiques au site sont prises en charge pour le mode routé qui utilise uniquement les EtherChannels étendus.

Les ID de site sont également utilisés pour permettre la mobilité de flux à l'aide de l'inspection LISP, la localisation du directeur pour améliorer les performances et réduire la latence aller-retour pour la mise en grappe inter-sites pour les centres de données, et la redondance des sites pour les connexions où un propriétaire de secours d'un flux se trouve toujours sur un autre site que celui du propriétaire.

Consultez les sections suivantes pour en savoir plus sur la mise en grappe inter-sites :

- Dimensionnement de l'interconnexion du centre de données : Exigences et conditions préalables à la mise en grappe sur Châssis Firepower 4100/9300 , à la page 452
- Lignes directrices inter-sites : Lignes directrices et limites de la mise en grappe, à la page 455
- Configurer la mobilité des flux de grappes : Configurer la mobilité des flux de grappes, à la page 484

- Activer la localisation du directeur : Activer la localisation du directeur, à la page 482
- Activer la redondance de site : Activer la localisation du directeur, à la page 482

Exigences et conditions préalables à la mise en grappe sur Châssis Firepower 4100/9300

Maximum d'unités de mise en grappe par modèle

- Firepower 4100 : 16 châssis
- Firepower 9300 : 16 modules. Par exemple, vous pouvez utiliser 1 module dans 16 châssis, ou 2 modules dans 8 châssis, ou toute combinaison qui fournit un maximum de 16 modules.

Exigences matérielles et logicielles pour la mise en grappe inter-châssis

Tous les châssis d'une grappe :

- : pour Firepower 4100 : tous les châssis doivent être du même modèle. Pour le périphérique Firepower 9300 : tous les modules de sécurité doivent être du même type. Par exemple, si vous utilisez la mise en grappe, tous les modules du périphérique Firepower 9300 doivent être des SM-40. Vous pouvez avoir différentes quantités de modules de sécurité installés dans chaque châssis, bien que tous les modules présents dans le châssis doivent appartenir à la grappe, y compris les logements vides.
- Doit exécuter FXOS et le logiciel d'application identiques, sauf au moment d'une mise à niveau d'image. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Doit inclure la même configuration d'interface pour les interfaces que vous affectez à la grappe, comme la même interface de gestion, les mêmes EtherChannels, les interfaces actives, la vitesse et le duplex, etc. Vous pouvez utiliser différents types de modules de réseau sur le châssis tant que les capacités correspondent pour les mêmes ID d'interface et que les interfaces peuvent être groupées avec succès dans le même EtherChannel étendu. Notez que toutes les interfaces de données doivent être des EtherChannels dans des grappes à plusieurs châssis. Si vous modifiez les interfaces dans FXOS après avoir activé la mise en grappe (en ajoutant ou en supprimant des modules d'interface, ou en configurant EtherChannels, par exemple), vous effectuez les mêmes modifications sur chaque châssis, en commençant par les nœuds de données jusqu'au nœud de contrôle.Notez que si vous supprimez une interface dans FXOS, la configuration de l'ASA conserve les commandes correspondantes afin que vous puissiez effectuer les ajustements nécessaires; la suppression d'une interface de la configuration peut avoir des effets importants. Vous pouvez supprimer manuellement l'ancienne configuration d'interface.
- Doit utiliser le même serveur NTP. Ne réglez pas l'heure manuellement.
- ASA : chaque châssis FXOS doit être enregistré auprès de l'autorité de licence ou du serveur satellite. Il n'y a pas de frais supplémentaires pour les nœuds de données. Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis. Pour Firewall Threat Defense, toutes les licences sont gérées par Firewall Management Center.

Exigences du commutateur

- Assurez-vous de terminer la configuration du commutateur et de connecter avec succès tous les canaux EtherChannels du châssis aux commutateurs avant de configurer la mise en grappe sur le Châssis Firepower 4100/9300 .
- Pour les caractéristiques de commutateur prises en charge, consultez Compatibilité Cisco FXOS.

dimensionnement de l'interconnexion du centre de données pour la mise en grappe inter-sites

Vous devez réserver la bande passante sur l'interconnexion des centres de données (DCI) pour un trafic de liaison de commande de grappe équivalent au calcul suivant :

$$\frac{\text{Nombre de membres de grappe par site}}{2} \times \text{liaison de commande de grappe par membre}$$

Si le nombre de membres diffère sur chaque site, utilisez le plus grand nombre pour votre calcul. La bande passante minimale pour l'interface DCI ne doit pas être inférieure à la taille de la liaison de commande de grappe pour un membre.

Par exemple :

- Pour 4 membres sur 2 sites :
  - 4 membres de la grappe au total
  - 2 membres sur chaque site
  - Liaison de commande de grappe de 5 Gbit/s par membre

  Bande passante DCI réservée = 5 Gbit/s (2/2 x 5 Gbit/s).
- Pour 6 membres sur 3 sites, la taille augmente :
  - Six membres de la grappe au total
  - 3 membres sur le site 1, 2 membres sur le site 2 et 1 membre sur le site 3
  - Liaison de commande de grappe de 10 Gbit/s par membre

  Bande passante DCI réservée = 15 Gbit/s (3/2 x 10 Gbit/s).
- Pour 2 membres sur 2 sites :
  - 2 membres de la grappe au total
  - Un membre sur chaque site
  - Liaison de commande de grappe de 10 Gbit/s par membre

  Bande passante DCI réservée = 10 Gbit/s (1/2 x 10 Gbit/s = 5 Gbit/s, mais la bande passante minimale ne doit pas être inférieure à la taille de la liaison de commande de grappe (10 Gbit/s)).

Licences pour la mise en grappe sur le Châssis Firepower 4100/9300

Smart Software Manager standard et sur site

La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence. Pour utiliser le cryptage renforcé et d'autres licences facultatives, chaque Châssis Firepower 4100/9300 doit être enregistré auprès de l'autorité de licence ou du serveur Smart Software Manager standard et sur site. Il n'y a pas de frais supplémentaires pour les unités de données.

La licence de cryptage renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement. Lors de l'utilisation du jeton, chaque châssis doit avoir la même licence de chiffrement. Pour la licence facultative de cryptage renforcé (3DES/AES) activée dans la configuration ASA, consultez ci-dessous.

Dans la configuration de la licence ASA, vous pouvez uniquement configurer la licence Smart sur l'unité de contrôle. La configuration est répliquée sur les unités de données, mais pour certaines licences, elles n'utilisent pas la configuration; elle reste dans un état mis en mémoire cache et seule l'unité de contrôle demande la licence. Les licences sont agrégées en une licence de grappe unique partagée par les unités de grappe, et cette licence agrégée est également mise en mémoire cache sur les unités de données pour être utilisée si l'une d'elles devient l'unité de contrôle ultérieurement. Chaque type de licence est géré comme suit :

- Essentials : seule l'unité de contrôle demande la licence Essentials au serveur et les deux unités peuvent l'utiliser en raison de l'agrégation des licences.
- Contexte : seule l'unité de contrôle demande la licence de contexte au serveur. La licence Essentials comprend 10 contextes par défaut et est présente sur tous les membres de la grappe. La valeur de la licence Essentials de chaque unité, plus la valeur de la licence de contexte sur l'unité de contrôle, sont combinées jusqu'à la limite de plateformes dans une licence de grappe agrégée. Par exemple :
  - Vous avez 6 modules Firepower 9300 dans la grappe. La licence Essentials comprend 10 contextes; pour 6 unités, ces licences ajoutent jusqu'à 60 contextes. Vous configurez une licence de 20 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 80 contextes. Comme la limite de plateformes pour un module est de 250, la licence combinée autorise un maximum de 250 contextes; les 80 contextes sont dans la limite. Par conséquent, vous pouvez configurer jusqu'à 80 contextes sur l'unité de contrôle; chaque unité de données aura également 80 contextes par la réplication de la configuration.
  - Vous avez 3 unités Firepower 4112 dans la grappe. La licence Essentials comprend 10 contextes; pour 3 unités, ces licences ajoutent jusqu'à 30 contextes. Vous configurez une licence de 250 contextes supplémentaires sur l'unité de contrôle. Par conséquent, la licence de grappe agrégée comprend 280 contextes. Comme la limite de plateformes pour une unité est de 250, la licence combinée autorise un maximum de 250 contextes; les 280 contextes sont au-dessus de la limite. Par conséquent, vous ne pouvez configurer que 250 contextes sur l'unité de contrôle; chaque unité de données aura également 250 contextes par la réplication de la configuration. Dans ce cas, vous devez uniquement configurer la licence de contexte de l'unité de contrôle pour 220 contextes.
- Opérateur : requis pour le VPN S2S distribué. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.
- Cryptage renforcé (3DES) : pour un déploiement Cisco Smart Software Manager sur site antérieur à la version 2.3.0, si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a

déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte. Cette licence est un droit par unité, et chaque unité demande sa propre licence au serveur.

Si une nouvelle unité de contrôle est choisie, la nouvelle unité de contrôle continue d'utiliser la licence agrégée. Elle utilise également la configuration de licence mise en mémoire cache pour demander à nouveau la licence de l'unité de contrôle. Lorsque l'ancienne unité de contrôle rejoint la grappe en tant qu'unité de données, elle libère le droit de licence de l'unité de contrôle. Avant que l'unité de données ne libère la licence, la licence de l'unité de contrôle peut être dans un état non conforme s'il n'y a aucune licence disponible dans le compte. La licence conservée est valide pendant 30 jours, mais si elle n'est toujours pas conforme après le délai de grâce, vous ne pourrez pas modifier la configuration des fonctionnalités nécessitant des licences spéciales; l'opération n'est pas affectée par le reste. La nouvelle unité active envoie une demande de renouvellement d'autorisation toutes les 12 heures jusqu'à ce que la licence soit conforme. Vous devez éviter de modifier la configuration jusqu'à ce que les demandes de licences soient complètement traitées. Si une unité quitte la grappe, la configuration de contrôle mise en mémoire cache est supprimée, tandis que les droits par unité sont conservés. En particulier, vous devrez demander à nouveau la licence de contexte sur les unités qui ne sont pas des grappes.

Réservation de licence permanente

Pour la réservation de licences permanentes, vous devez acheter des licences distinctes pour chaque châssis et activer les licences *avant* de configurer la mise en grappe.

Lignes directrices et limites de la mise en grappe

Commutateurs pour la mise en grappe

- Assurez-vous que les commutateurs connectés correspondent aux unités de transfert maximales MTU des interfaces de données et de l'interface de liaison de commande de grappe. Vous devez configurer la MTU de l'interface de la liaison de commande de grappe pour qu'elle soit au moins 100 octets supérieure à la MTU de l'interface de données. Assurez-vous donc de configurer le commutateur de connexion de la liaison de commande de grappe correctement. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe. De plus, nous ne conseillons pas de définir la MTU de la liaison de commande de grappe entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système.
- Pour les systèmes Cisco IOS XR, si vous souhaitez définir une MTU autre que celle par défaut, définissez la MTU de l'interface IOS XR sur 14 octets au-dessus de la MTU du périphérique de la grappe. Sinon, les tentatives d'homologation de contiguïté OSPF peuvent échouer, sauf si l'option **mtu-ignore** est utilisée. Notez que la MTU du périphérique de grappe doit correspondre à la MTU *IPv4* d'IOS XR. Cet ajustement n'est pas nécessaire pour les commutateurs Cisco Catalyst et Cisco Nexus.
- Sur le ou les commutateurs pour les interfaces de liaison de commande de grappe, vous pouvez éventuellement activer Spanning Tree PortFast sur les ports de commutateur connectés à l'unité de la grappe pour accélérer le processus de jonction des nouvelles unités.
- Sur le commutateur, nous vous conseillons d'utiliser l'un des algorithmes d'équilibrage de charges EtherChannel suivants : **source-dest-ip** or **src-dst-mixed-ip-port** (reportez-vous à la commande **port-channel load-balance** de Cisco Nexus OS et Cisco IOS-XE). N'utilisez pas de mot clé **vlan** dans l'algorithme d'équilibrage de charge, car cela pourrait entraîner une répartition inégale du trafic vers les

périphériques d'une grappe. *Ne modifiez pas* l'algorithme d'équilibrage de charge par défaut sur le périphérique de la grappe.

- Si vous modifiez l'algorithme d'équilibrage de charge de l'EtherChannel sur le commutateur, l'interface EtherChannel du commutateur arrête temporairement de transférer le trafic et le protocole Spanning Tree redémarre. Il faudra attendre un certain temps avant que le trafic ne redevienne fluide.
- Les commutateurs sur le chemin de la liaison de commande de grappe ne doivent pas vérifier la somme de contrôle L4. Le trafic redirigé sur la liaison de commande de grappe n'a pas une somme de contrôle L4 correcte. Les commutateurs qui vérifient la somme de contrôle L4 pourraient entraîner l'abandon du trafic.
- Le temps d'arrêt du groupage du canal de port ne doit pas dépasser l'intervalle Keepalive configuré.
- Sur les EtherChannels de 2e génération, l'algorithme de distribution de hachage par défaut est adaptatif. Pour éviter le trafic symétrique dans une conception VSS, modifiez l'algorithme de hachage sur le canal de port connecté au périphérique de la grappe à fixe :

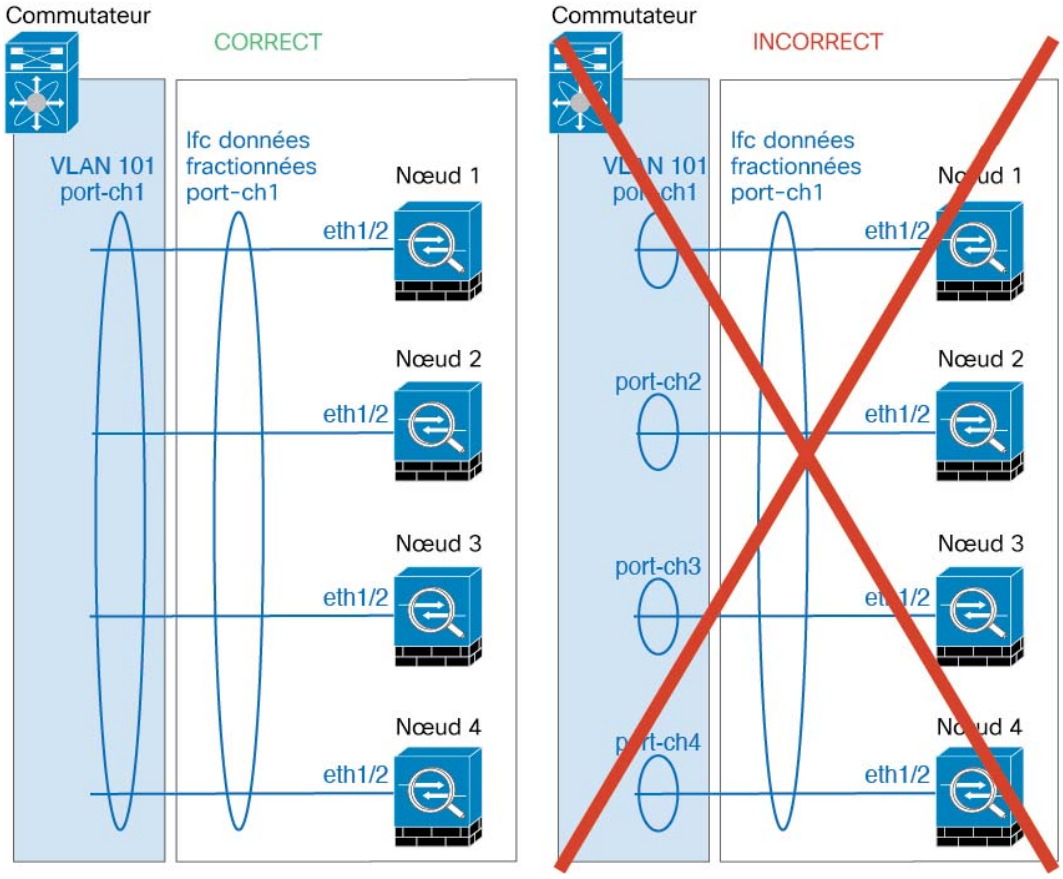
  router(config)# **port-channel** *id* **hash-distribution fixed**

  Ne modifiez pas l'algorithme globalement; vous pouvez profiter de l'algorithme adaptatif pour la liaison homologue VSS.

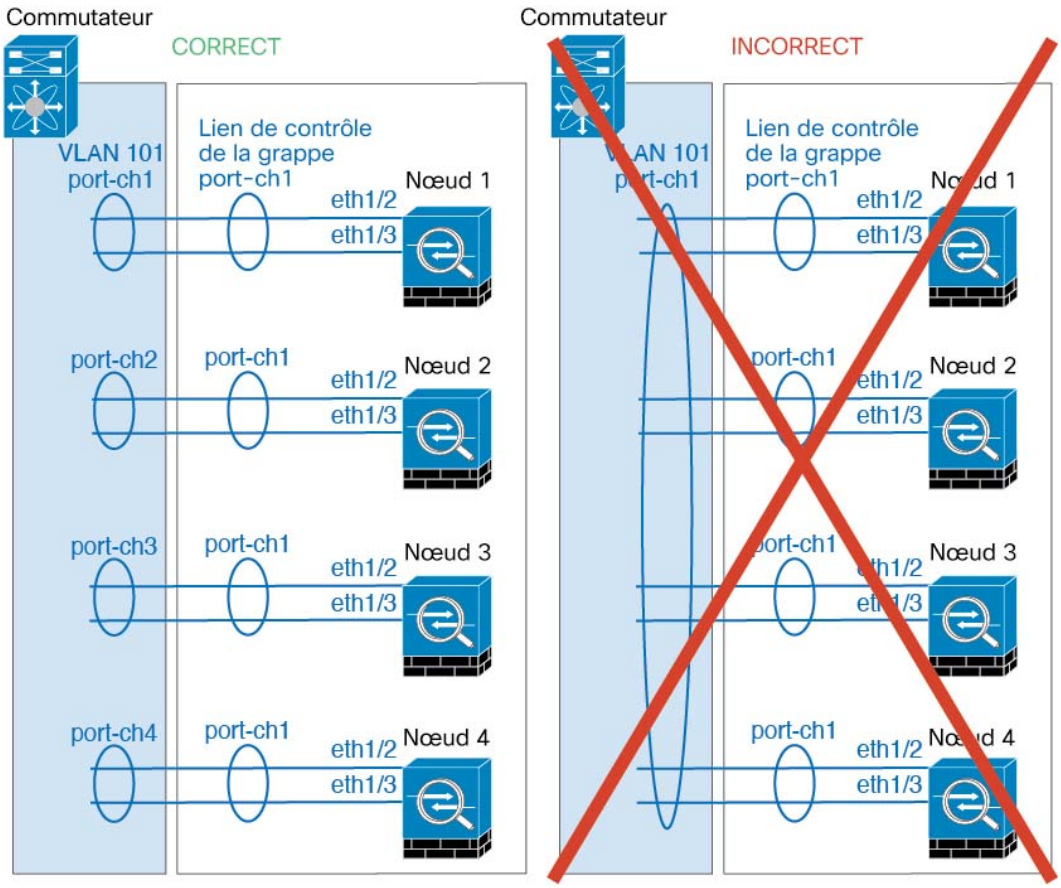
- Contrairement aux grappes de matériel ASA, les grappes Firepower 4100/9300 prennent en charge la convergence progressive LACP. Ainsi, pour la plateforme, vous pouvez laisser la convergence progressive LACP activée sur les commutateurs Cisco Nexus connectés.
- Lorsque vous voyez le regroupement lent d'un EtherChannel étendu sur le commutateur, vous pouvez activer un débit LACP rapide pour une interface individuelle sur le commutateur. Le débit du protocole LACP de FXOS EtherChannels est rapide par défaut. Notez que certains commutateurs, comme la série Nexus, ne prennent pas en charge le débit LACP rapide lors des mises à niveau logicielles en service (ISSU). Nous ne recommandons donc pas l'utilisation des ISSU avec la mise en grappe.

EtherChannels pour la mise en grappe

- Dans les versions du logiciel Cisco IOS Catalyst 3750-X antérieures à la15.1(1)S2, l'unité de grappe ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel de l'unité de grappe est connecté de manière croisée et si le commutateur de l'unité de contrôle est hors tension, l'EtherChannel connecté au commutateur restant ne s'activera pas. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.
- Configuration des EtherChannels étendus vs. locaux au périphérique : veillez à configurer le commutateur de manière appropriée pour les EtherChannels étendus par rapport aux EtherChannels locaux au périphérique.
  - EtherChannels étendus : pour les EtherChannels *étendus* des unités de grappe, qui s'étendent sur tous les membres de la grappe, les interfaces sont combinées en un seul EtherChannel sur le commutateur. Vérifiez que chaque interface se trouve dans le même groupe de canaux sur le commutateur.



- EtherChannels locaux au périphérique : pour les EtherChannels *locaux au périphérique* de grappe, y compris tous les EtherChannels configurés pour la liaison de commande de la grappe, veillez à configurer des EtherChannels isolés sur le commutateur; ne combinez pas plusieurs EtherChannels d'unités de grappe en un seul EtherChannel sur le commutateur.



Mise en grappe inter-sites

Consultez les consignes suivantes concernant la mise en grappe inter-sites :

- La latence de la liaison de commande de grappe doit être inférieure à 20 ms temps aller-retour (RTT).
- La liaison de commande de grappe doit être fiable, sans paquets dans le désordre ou abandonnés; par exemple, vous devez utiliser un lien dédié.
- Ne configurez pas le rééquilibrage de connexion; il ne faut pas que les connexions soient rééquilibrées entre les membres de la grappe sur un site différent.
- Le ASA ne chiffre pas le trafic de données transféré sur la liaison de commande de grappe, car il s'agit d'un lien dédié, même lorsqu'il est utilisé sur une interconnexion de centre de données (DCI). Si vous utilisez la virtualisation du transport par superposition (OTV), ou étendez la liaison de commande de grappe en dehors du domaine administratif local, vous pouvez configurer le chiffrement sur vos routeurs de frontière, comme 802.1AE MacSec sur OTV.
- La mise en œuvre de la grappe ne fait pas de différence entre les membres de plusieurs sites pour les connexions entrantes; par conséquent, les rôles de connexion pour une connexion donnée peuvent s'étendre sur plusieurs sites. Il s'agit du comportement attendu. Toutefois, si vous activez la localisation de directeur, le rôle de directeur local est toujours choisi sur le même site que le propriétaire de la connexion (selon l'ID du site). En outre, le directeur local choisit un nouveau propriétaire sur le même site si le propriétaire d'origine tombe en panne (Remarque : si le trafic est dissymétrique entre les sites et qu'il y a un trafic

continu en provenance du site distant après la défaillance du propriétaire d'origine, alors un nœud du site distant site peut devenir le nouveau propriétaire s'il reçoit un paquet de données pendant la fenêtre de réhébergement.).

- Pour la localisation du directeur, les types de trafic suivants ne prennent pas en charge la localisation : le trafic NAT ou PAT; trafic inspecté par SCTP; requête du propriétaire de la fragmentation.
- Dans un déploiement Nord-Sud avec des flux UDP persistants, des boucles de routage peuvent se produire si les nœuds du site propriétaire initial du flux tombent en panne, puis reviennent en ligne, ce qui entraîne une redirection du flux vers le site d'origine. Si le nouveau propriétaire, sur l'autre site, ne dispose pas d'une route vers la destination, il redirigera le flux vers Internet, créant ainsi une boucle. Dans ce cas, utilisez la commande **clear conn** sur le nouveau propriétaire pour forcer la réinitialisation du flux.
- Pour le mode transparent, si la grappe est placée entre une paire de routeurs internes et externes (AKA insertion nord-sud), vous devez vous assurer que les deux routeurs internes partagent une adresse MAC et que les deux routeurs externes partagent une adresse MAC. Lorsqu'un membre de la grappe sur le site 1 transfère une connexion à un membre du site 2, l'adresse MAC de destination est conservée. Le paquet n'atteindra le routeur du site 2 que si l'adresse MAC est la même que celle du routeur du site 1.
- Pour le mode transparent, si la grappe est placée entre les réseaux de données et le routeur de passerelle de chaque site pour le pare-feu entre les réseaux internes (AKA insertion est-ouest), chaque routeur de passerelle doit utiliser un protocole FHRP (First Hop Redundancy Protocol) comme HSRP pour fournir des destinations d'adresses IP et MAC virtuelles identiques sur chaque site. Les VLAN de données sont étendus à l'ensemble des sites à l'aide de la virtualisation du transport par superposition (OTV), ou d'un outil similaire. Vous devez créer des filtres pour empêcher le trafic destiné au routeur de la passerelle local d'être envoyé à l'autre site sur DCI. Si le routeur de la passerelle devient inaccessible sur un site, vous devez supprimer les filtres pour que le trafic puisse atteindre la passerelle de l'autre site.
- Pour le mode transparent, si la grappe est connectée à un routeur HSRP, vous devez ajouter l'adresse MAC HSRP du routeur en tant qu'entrée de tableau d'adresses MAC statiques sur ASA (voir Ajouter une adresse MAC statique pour les groupes de ponts, à la page 929). Lorsque des routeurs adjacents utilisent HSRP, le trafic destiné à l'adresse IP HSRP sera envoyé à l'adresse MAC HSRP, mais le trafic retour proviendra de l'adresse MAC de l'interface d'un routeur particulier dans la paire HSRP. Par conséquent, le tableau d'adresses MAC ASA n'est généralement mis à jour que lorsque l'entrée du tableau ARP ASA pour l'adresse IP HSRP expire et que le ASA envoie une demande ARP et reçoit une réponse. Étant donné que les entrées du tableau ARP de ASAexpirent après 14 400 secondes par défaut, mais que l'entrée du tableau d'adresses MAC expire après 300 secondes par défaut, une entrée d'adresse MAC statique est requise pour éviter les pertes de trafic liées à l'expiration du tableau.
- Pour le mode routé à l'aide de l'EtherChannel étendu, configurez les adresses MAC propres au site. Étendre les VLAN de données à tous les sites à l'aide d'OTV ou d'un outil similaire. Vous devez créer des filtres pour empêcher le trafic destiné à l'adresse MAC globale d'être envoyé à l'autre site par DCI. Si la grappe devient inaccessible sur un site, vous devez supprimer les filtres pour que le trafic puisse atteindre les nœuds de la grappe de l'autre site. Le routage dynamique n'est pas pris en charge lorsqu'une grappe inter-sites sert de routeur de premier saut pour un segment étendu.

Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'Châssis Firepower 4100/9300 ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise, ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les

interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.

- lors de l'ajout d'une unité à une grappe existante ou lors du rechargement d'une unité, il se produira une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent suspendre les connexions; Par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Si vous utilisez un serveur Windows 2003 connecté à une interface EtherChannel étendue, lorsque le port du serveur syslog est en panne et que le serveur ne limite pas les messages d'erreur ICMP, un grand nombre de messages ICMP sont renvoyés à la grappe. Ces messages peuvent faire en sorte que certaines unités de la grappe connaissent un niveau élevé de CPU, ce qui peut affecter les performances. Nous vous recommandons de limiter les messages d'erreur ICMP.
- Nous vous recommandons de connecter les EtherChannels à un VSS, à un vPC, à StackWise ou à StackWise Virtual pour la redondance.
- Dans un châssis, vous ne pouvez pas mettre en grappe certains modules de sécurité et exécuter d'autres modules de sécurité en mode autonome; vous devez inclure tous les modules de sécurité dans la grappe.

Valeurs par défaut

- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- Le rééquilibrage de la connexion est désactivé par défaut. Si vous activez le rééquilibrage de la connexion, l'intervalle par défaut entre les échanges d'informations de chargement est de 5 secondes.
- La fonction de jonction automatique de la grappe pour une liaison de commande de grappe défaillante est définie pour permettre un nombre illimité de tentatives toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante est définie à 3 tentatives toutes les 5 minutes, avec un intervalle croissant défini à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe sur le Châssis Firepower 4100/9300

Vous pouvez facilement déployer la grappe à partir du superviseur Châssis Firepower 4100/9300 . Toute la configuration initiale est générée automatiquement pour chaque unité. Cette section décrit la configuration du démarrage par défaut et la personnalisation facultative que vous pouvez effectuer sur l'ASA. Cette section décrit également comment gérer les membres de la grappe à partir de l'ASA. Vous pouvez également gérer l'appartenance à la grappe à partir du Châssis Firepower 4100/9300 . Pour obtenir de plus amples renseignements, consultez la documentation du Châssis Firepower 4100/9300 .

Procédure

Étape 1 FXOS : Ajouter une grappe ASA, à la page 461

Étape 2 ASA : Modifier le mode de pare-feu et le mode de contexte, à la page 471

Étape 3 ASA : Configurer les interfaces de données, à la page 472

Étape 4 ASA : Personnaliser la configuration de la grappe, à la page 475

Étape 5 ASA : Gérer les membres de la grappe, à la page 497

FXOS : Ajouter une grappe ASA

Vous pouvez ajouter un seul châssis Firepower 9300 en tant que grappe intra-châssisou ajouter plusieurs châssis pour la mise en grappe inter-châssis. Pour la mise en grappe inter-châssis, vous devez configurer chaque châssis séparément. Ajoutez la grappe sur un châssis; vous pouvez ensuite saisir la plupart des mêmes paramètres sur le châssis suivant.

Créer une grappe ASA

Définissez la portée sur la version de l'image.

Vous pouvez facilement déployer la grappe à partir du superviseur Châssis Firepower 4100/9300 . Toute la configuration initiale est générée automatiquement pour chaque unité.

Pour la mise en grappe sur plusieurs châssis, vous devez configurer chaque châssis séparément. Déployer la grappe sur un châssis; vous pouvez ensuite copier la configuration de démarrage du premier châssis au châssis suivant pour faciliter le déploiement.

Dans un châssis Firepower 9300, vous devez activer la mise en grappe pour les 3 logements de module , même si aucun module n'est installé. Si vous ne configurez pas les 3 modules, la grappe ne s'affichera pas.

Pour le mode à contextes multiples, vous devez d'abord déployer le périphérique logique, puis activer le mode à contextes multiples dans l'application ASA.

Lorsque vous déployez une grappe, le superviseur Châssis Firepower 4100/9300 configure chaque application ASA avec la configuration de démarrage suivante. Vous pouvez modifier ultérieurement, si vous le souhaitez, des parties de la configuration de démarrage à partir de l'ASA (en **gras**).

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>
   site-id <number>
   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
   enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
   management-only individual
   nameif management
   security-level 0
   ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
   no shutdown

http server enable
```

```
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```



Remarque Le nom **local-unit** ne peut être modifié que si vous désactivez la mise en grappe.

Avant de commencer

- Téléchargez l'image de l'application que vous voulez utiliser pour l'appareil logique à partir de Cisco.com, puis téléchargez cette image sur le serveur de l'application Châssis Firepower 4100/9300 .
- Recueillez les informations suivantes :
  - ID de l'interface de gestion, adresses IP et masque de réseau
  - Adresse IP de la passerelle

Procédure

Étape 1 Configurer les interfaces.

a) Ajoutez au moins une interface de type de données ou un EtherChannel (également appelé canal de port) avant de déployer la grappe. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port), à la page 183 ou Configurer une interface physique, à la page 181.

Pour la mise en grappe sur plusieurs châssis, toutes les interfaces de données doivent être des EtherChannels étendus avec au moins une interface membre. Ajoutez les mêmes EtherChannels sur chaque châssis. Combinez les interfaces membres de toutes les unités de la grappe en un seul EtherChannel sur le commutateur. Consultez Lignes directrices et limites de la mise en grappe, à la page 455 pour obtenir des renseignements sur les EtherChannels.

b) Ajoutez une interface de type de gestion ou un EtherChannel. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port), à la page 183 ou Configurer une interface physique, à la page 181.

L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que l'interface de gestion du châssis qui est utilisée uniquement pour la gestion de ce dernier (dans FXOS, vous pouvez voir l'interface de gestion du châssis affichée comme MGMT, management0, ou d'autres noms similaires).

Pour la mise en grappe sur plusieurs châssis, ajoutez la même interface de gestion sur chaque châssis.

c) Pour la mise en grappe sur plusieurs châssis, ajoutez une interface membre à l'EtherChannel de la liaison de commande de grappe (par défaut, le canal de port 48). Consultez Ajouter un canal EtherChannel (canal de port), à la page 183.

N'ajoutez pas d'interface membre pour une grappe isolée aux modules de sécurité dans un châssis Firepower 9300. Si vous ajoutez un membre, le châssis suppose que cette grappe utilisera plusieurs châssis et vous permettra uniquement d'utiliser des EtherChannels étendus, par exemple.

Ajoutez les mêmes interfaces membre sur chaque châssis. La liaison de commande de grappe est un EtherChannel local au périphérique sur chaque châssis. Utilisez des EtherChannels distincts sur le commutateur pour chaque périphérique. Consultez Lignes directrices et limites de la mise en grappe, à la page 455 pour obtenir des renseignements sur les EtherChannels.

Étape 2 Entrez le mode de services de sécurité.

scope ssa

Exemple :

```
Firepower# scope ssa
Firepower /ssa #
```

Étape 3 Définissez les paramètres d'instance de l'application, y compris la version de l'image.

a) Affichez les images disponibles. Notez le numéro de version que vous souhaitez utiliser.

show app

Exemple :

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) Définissez la portée sur la version de l'image.

scope app asa *application_version*

Exemple :

```
Firepower /ssa # scope app asa 9.10.1
Firepower /ssa/app #
```

c) Définissez cette version comme étant la version par défaut.

set-default

Exemple :

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) Quittez le mode ssa.

exit

Exemple :

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

Exemple :

```
Firepower /ssa # scope app asa 9.12.1
```

```
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

Étape 4 Créer la grappe.

enter logical-device *device_name* **asa** *slots* **clustered**

- *device_name :*utilisé par le superviseur Châssis Firepower 4100/9300 pour configurer les paramètres de mise en grappe et affecter des interfaces; il ne s'agit pas du nom de grappe utilisé dans la configuration du module de sécurité. Vous devez préciser les trois modules de sécurité, même si vous n'avez pas encore installé le matériel.
- *slots (logements)* : attribue les modules de châssis à la grappe. Pour Firepower 4100, spécifiez **1**. Pour Firepower 9300, spécifiez **1,2,3**. Vous devez activer la mise en grappe pour les 3 logements de module dans un châssis Firepower 9300, même si aucun module n'est installé. Si vous ne configurez pas les 3 modules, la grappe ne s'affichera pas.

Exemple :

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

Étape 5 Configurer les paramètres de démarrage de la grappe.

Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

a) Créez l'objet de démarrage de grappe.

enter cluster-bootstrap

Exemple :

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) Définissez l'ID de châssis.

set chassis-id *ID*

Chaque châssis de la grappe a besoin d'un ID unique.

c) Pour la mise en grappe inter-sites, définissez l'ID de site entre 1 et 8.

set site-id *nombre*.

Pour supprimer l'ID de site, définissez la valeur à **0**.

Exemple :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) Configurez une clé d'authentification pour contrôler le trafic dans la liaison de commande de la grappe.

set key

Exemple :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

Vous êtes invité à saisir le code secret partagé.

Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le code secret partagé est utilisé pour générer la clé de chiffrement. Cette option n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair.

e) Définissez le mode d'interface de grappe.

set mode spanned-etherchannel

Le mode EtherChannel étendu est le seul mode pris en charge.

Exemple :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

f) Définissez le nom du groupe de grappes dans la configuration du module de sécurité.

set service-type *nom_grappe*

Le nom doit être une chaîne ASCII comptant de 1 à 38 caractères.

Exemple :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

g) (Facultatif) Définissez le réseau IP de la liaison de commande de la grappe.

set cluster-control-link network *a*.*b*.**0.0**

Par défaut, la liaison de commande de grappe utilise le réseau 127.2.0.0/16. Cependant, certains déploiements réseau ne permettent pas le passage du trafic 127.2.0.0/16. Dans ce cas, vous pouvez spécifier une adresse /16 sur un réseau unique pour la grappe.

- *a*.*b*.**0.0** : spécifiez toute adresse réseau /16, à l'exception des adresses de boucle avec retour (127.0.0.0/8) et de multidiffusion (224.0.0.0/4). Si vous définissez la valeur à 0.0.0.0, le réseau par défaut est utilisé : 127.2.0.0.

Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID de logement : *a*.*b*.*id_châssis*.*id_logement*.

Exemple :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
10.10.0.0
```

h) Configurez les informations relatives à l'adresse IP de gestion.

Ces informations sont utilisées pour configurer une interface de gestion dans la configuration du module de sécurité.

1. Configurez un ensemble d'adresses IP locales, dont une sera affectée à chaque unité de grappe pour l'interface.

   set ipv4 pool *start_ip end_ip*

   set ipv6 pool *start_ip end_ip*

   Incluez au moins autant d'adresses qu'il y a d'unités dans la grappe. Notez que pour le périphérique Firepower 9300, vous devez inclure 3 adresses par châssis, même si tous les logements de module ne sont pas remplis. Si vous prévoyez d'étendre la grappe, incluez des adresses supplémentaires. L'adresse IP virtuelle (appelée adresse IP de la grappe principale) qui appartient à l'unité de contrôle actuelle ne fait *pas* partie de cet ensemble; Assurez-vous de réserver une adresse IP sur le même réseau pour l'adresse IP de la grappe principale. Vous pouvez utiliser des adresses IPv4 et/ou IPv6.

2. Configurez l'adresse IP de l'ensemble d'adresses principal pour l'interface de gestion.

   set virtual ipv4 *ip_address* **mask** *mask*

   set virtual ipv6 *ip_address* **prefix-length** *prefix*

   Cette adresse IP doit être sur le même réseau que les adresses de l'ensemble d'adresses de la grappe, mais ne doit pas faire partie de ce dernier.

3. Saisissez l'adresse de la passerelle du réseau.

   set ipv4 gateway *ip_address*

   set ipv6 gateway *ip_address*

Exemple :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

i) Quittez le mode de démarrage de la grappe.

   exit

Exemple :

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

Étape 6 Configurez les paramètres de démarrage de gestion.

Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

a) Créez l'objet de démarrage de gestion.

enter mgmt-bootstrap asa

Exemple :

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) Spécifiez le mot de passe d'administrateur et d'activation.

create bootstrap-key-secret PASSWORD

set value

Saisissez une valeur *mot de passe*

Confirmez la valeur : *mot de passe*

exit

Exemple :

L'utilisateur admin ASA et le mot de passe d'activation préconfigurés sont utiles pour la récupération du mot de passe. si vous avez un accès FXOS, vous pouvez réinitialiser le mot de passe de l'utilisateur admin en cas d'oubli.

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) Spécifiez le mode de pare-feu, routage ou transparent.

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

En mode routage, l'appareil est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) Quittez le mode de démarrage de gestion.

exit

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Étape 7 Enregistrez la configuration.

commit-buffer

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Vérifiez l'état du déploiement à l'aide de la commande **show app-instance**. L'instance d'application est en cours d'exécution et prête à être utilisée lorsque l'état **Admin State** est **Enabled** (Activé) et que l'état **Oper State** est **Online** (En ligne).

Exemple :

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- ------------
ftd        cluster1   1          Enabled     Online           7.3.0.49        7.3.0.49
    Native                   In Cluster      Data Node
ftd        cluster1   2          Enabled     Online           7.3.0.49        7.3.0.49
    Native                   In Cluster      Control Node
ftd        cluster1   3          Disabled    Not Available                    7.3.0.49
    Native                   Not Applicable  None
```

Étape 8 Pour ajouter un autre châssis à la grappe, répétez cette procédure, sauf que vous devez configurer un unique **chassis-id** et le bon **site-id**; Sinon, utilisez la même configuration pour les deux châssis.

Vérifiez que la configuration de l'interface est la même sur le nouveau châssis. Vous pouvez exporter et importer la configuration du châssis FXOS pour faciliter ce processus.

Étape 9 Connectez-vous à l'unité de contrôle ASA pour personnaliser votre configuration de mise en grappe.

Exemple

Pour le châssis 1 :

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      enter member-port Ethernet1/1
```

```
        exit
      enter member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

Pour le châssis 2 :

```
scope eth-uplink
  scope fabric a
```

```
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      create member-port Ethernet2/2
        exit
      exit
    create port-channel 48
      set port-type cluster
      enable
      create member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.15
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::19
      set key
      Key: f@rscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

Ajouter d'autres membres à la grappe

Ajoutez ou remplacez le membre de la grappe ASA.

Remarque Cette procédure s'applique uniquement à l'ajout ou au remplacement d'un *châssis*; si vous ajoutez ou remplacez un module sur un Firepower 9300 pour lequel la mise en grappe est déjà activée, le module sera ajouté automatiquement.

Avant de commencer

- Assurez-vous que votre grappe existante dispose d'un nombre suffisant d'adresses IP dans l'ensemble d'adresses IP de gestion pour ce nouveau membre. Sinon, vous devez modifier la configuration de démarrage de grappe existante sur chaque châssis avant d'ajouter ce nouveau membre. Cette modification entraîne le redémarrage du périphérique logique.
- La configuration de l'interface doit être la même sur le nouveau châssis. Vous pouvez exporter et importer la configuration du châssis FXOS pour faciliter ce processus.
- Pour le mode de contexte multiple, activez le mode de contexte multiple dans l'application ASA sur le premier membre de grappe; les membres de la grappe héritent automatiquement de la configuration en mode de contexte multiple.

Procédure

Étape 1 cliquez sur **OK**.

Étape 2 Pour ajouter un autre châssis à la grappe, répétez la procédure dans Créer une grappe ASA, à la page 461, sauf que vous devez configurer un **chassis-id** unique et le bon **site-id**; sinon, utilisez la même configuration pour le nouveau châssis.

ASA : Modifier le mode de pare-feu et le mode de contexte

Par défaut, le châssis FXOS déploie une grappe en mode de pare-feu routé et en mode de contexte unique.

- Changer le mode de pare-feu : pour changer le mode après le déploiement, changez le mode sur l'unité de contrôle; le mode est automatiquement modifié sur toutes les unités de données pour qu'elles correspondent. Consultez Définir le mode du pare-feu, à la page 210. En mode de contexte multiple, vous définissez le mode de pare-feu par contexte.Consultez le
- Passer en mode de contexte multiple : pour passer en mode de contexte multiple après le déploiement, modifiez le mode sur l'unité de contrôle; le mode est automatiquement modifié sur toutes les unités de données pour qu'elles correspondent. Voir Activer le mode de contexte multiple, à la page 240.Consultez le

ASA : Configurer les interfaces de données

Cette procédure configure les paramètres de base pour chaque interface de données que vous avez affectée à la grappe lorsque vous l'avez déployée dans FXOS. Pour la mise en grappe sur plusieurs châssis, les interfaces de données sont toujours des interfaces EtherChannel étendus.



Remarque L'interface de gestion a été préconfigurée lorsque vous avez déployé la grappe. Vous pouvez également modifier les paramètres de l'interface de gestion dans l'ASA, mais cette procédure se concentre sur les interfaces de données. L'interface de gestion est une interface individuelle spéciale, par opposition à une interface étendue. Consultez Interface de gestion, à la page 449 pour de plus amples renseignements.

Avant de commencer

- Pour le mode de contexte multiple, commencez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.
- Pour le mode transparent, configurez le groupe de ponts. Consultez Configurer la BVI (Bridge Virtual Interface), à la page 772.
- Lorsque vous utilisez des EtherChannels étendus pour une grappe avec plusieurs châssis, l'interface du canal de port ne s'affiche pas tant que la mise en grappe n'est pas complètement activée. Cette exigence empêche le trafic d'être transféré vers un nœud qui n'est pas un nœud actif dans la grappe.

Procédure

Étape 1 Spécifiez l'ID de l'interface.

interface *ID*

Reportez-vous au châssis FXOS pour connaître les interfaces attribuées à cette grappe. L'ID d'interface peut être :

- **canal de port** *entier*
- **ethernet** *logement/port*

Exemple :

```
ciscoasa(config)# interface port-channel 1
```

Étape 2 Activez l'interface :

no shutdown

Étape 3 (Facultatif) Si vous créez des sous-interfaces VLAN sur cette interface, faites-le maintenant.

Exemple :

```
ciscoasa(config)# interface port-channel 1.10
```

```
ciscoasa(config-if)# vlan 10
```

Le reste de cette procédure s'applique aux sous-interfaces.

Étape 4 (Mode de contexte multiple) Affectez l'interface à un contexte, puis changez de contexte et passez en mode d'interface.

Exemple :

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

Pour le mode de contexte multiple, le reste de la configuration d'interface se produit dans chaque contexte.

Étape 5 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif inside
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur.

Étape 6 Effectuez l'une des opérations suivantes, selon le mode de pare-feu.

- Mode routé : définissez l'adresse IPv4 et/ou IPv6 :

  (IPv4)

  ip address *ip_address* [*mask*]

  (IPv6)

  ipv6 address *ipv6-prefix*/*prefix-length*

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

  Les configurations automatiques DHCP, PPPoE et IPv6 ne sont pas prises en charge. Pour les connexions point à point, vous pouvez spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. La configuration manuelle de l'adresse Link-Local n'est pas non plus prise en charge.

- Mode transparent : affectez l'interface à un groupe de ponts :

  bridge-group *number*

  Exemple :

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

Où *le nombre* est un entier compris entre 1 et 100. Vous pouvez attribuer jusqu'à 64 interfaces à un groupe de ponts. Vous ne pouvez pas attribuer la même interface à plusieurs groupes de ponts. Notez que la configuration des BVI comprend l'adresse IP.

Étape 7 Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Où *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 8 (Mise en grappe sur plusieurs châssis) Configurez une adresse MAC globale unique et manuelle pour un EtherChannel étendu afin d'éviter d'éventuels problèmes de connectivité au réseau.

mac-address *mac_address*

- *mac_address* : l'adresse MAC est au format H.H.H., où H est une valeur hexadécimale de 16 bits. Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE est saisie comme suit : 000C.F142.4CDE. Les deux premiers octets d'une adresse MAC manuelle ne peuvent pas être A2 si vous souhaitez également utiliser des adresses MAC générées automatiquement.

Vous devez configurer une adresse MAC unique qui n'est pas utilisée actuellement sur votre réseau. Dans le cas d'une adresse MAC configurée manuellement, l'adresse MAC reste celle de l'unité de contrôle actuelle. Si vous ne configurez pas d'adresse MAC, si l'unité de contrôle change, la nouvelle unité de contrôle utilisera une nouvelle adresse MAC pour l'interface, ce qui peut provoquer une panne temporaire du réseau.

En mode de contexte multiple, si vous partagez une interface entre les contextes, vous devez plutôt activer la génération automatique des adresses MAC pour ne pas avoir à définir l'adresse MAC manuellement. Notez que vous devez configurer manuellement l'adresse MAC à l'aide de cette commande pour les interfaces *non partagées*.

Exemple :

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

Étape 9 (Mise en grappe inter-sites) Configurez une adresse MAC spécifique au site et, pour le mode routé, une adresse IP pour chaque site :

mac-address *mac_address* **site-id** *number* **site-ip** *ip_address*

Exemple :

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

Les adresses IP spécifiques au site doivent se trouver sur le même sous-réseau que l'adresse IP globale. L'adresse MAC spécifique au site et l'adresse IP utilisées par une unité dépendent de l'ID de site que vous spécifiez dans la configuration de démarrage de chaque unité.

ASA : Personnaliser la configuration de la grappe

Si vous souhaitez modifier les paramètres de démarrage après avoir déployé la grappe ou configuré des options supplémentaires, comme la surveillance de l'intégrité de la grappe, le délai de réplication de la connexion TCP, la mobilité des flux et d'autres optimisations, vous pouvez le faire sur l'unité de contrôle.

Configurer les paramètres de grappe ASA de base

Vous pouvez personnaliser les paramètres de grappe sur le nœud de contrôle.

Avant de commencer

- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système sur l'unité de contrôle. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.
- Le nom de l'unité locale et plusieurs autres options ne peuvent être définis que sur le châssis FXOS, ou ils ne peuvent être modifiés que sur l'ASA si vous désactivez la mise en grappe. Ils ne sont donc pas inclus dans la procédure suivante.

Procédure

Étape 1 Confirmez qu'il s'agit de l'unité de contrôle :

show cluster info

Exemple :

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state CONTROL_NODE
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state DATA_NODE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
```

```
    Last leave: 20:24:55 UTC Nov 4 2015
Unit "unit-1-1" in state DATA_NODE
    ID        : 1
    Version   : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.1.1
    CCL MAC   : 0015.c500.017f
    Last join : 20:20:53 UTC Nov 4 2015
    Last leave: 20:18:15 UTC Nov 4 2015
Unit "unit-2-1" in state DATA_NODE
    ID        : 3
    Version   : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.2.1
    CCL MAC   : 0015.c500.020f
    Last join : 20:19:57 UTC Nov 4 2015
    Last leave: 20:24:55 UTC Nov 4 2015
```

Si une autre unité est l'unité de contrôle, quittez la connexion et connectez-vous à l'unité appropriée.

Étape 2 Spécifiez l'unité de transfert maximale de l'interface de liaison de commande de grappe, qui doit être supérieure d'au moins 100 octets à la MTU la plus élevée des interfaces de données.

mtu cluster *bytes*

Exemple :

```
ciscoasa(config)# mtu cluster 9184
```

Nous vous suggérons de définir la MTU de la liaison de commande de grappe au maximum; la valeur minimale est de 1 400 octets. De plus, nous ne conseillons pas de définir la MTU de la liaison de commande de grappe entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe. Par exemple, comme la MTU maximale est de 9 184 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9 084 octets, tandis que la liaison de commande de grappe peut être définie sur 9 184 octets.

Étape 3 Entrez en mode de configuration de la grappe :

cluster group *name*

Étape 4 (Facultatif) Activez la réplication de la console des unités de données vers l'unité de contrôle :

console-replicate

Par défaut, cette fonction est désactivée. L'ASA imprime certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de console, les unités de données envoient les messages de console à l'unité de contrôle de sorte qu'il suffit de surveiller un seul port de console pour la grappe.

Étape 5 Définissez le niveau de trace minimal pour les événements de mise en grappe :

trace-level *level*

Définissez le niveau minimum comme souhaité :

- **critical**—Événements critiques (gravité=1)
- **warning**—Avertissements (gravité=2)

- **informational**—Événements informationnels (gravité=3)
- **debug**—Événements de débogage (gravité= 4)

Étape 6 (Facultatif) (Firepower 9300 uniquement) Assurez-vous que les modules de sécurité d'un châssis rejoignent la grappe simultanément afin que le trafic soit réparti uniformément entre les modules. Si un module se joint très avant les autres modules, il peut recevoir plus de trafic que souhaité, car les autres modules ne peuvent pas encore partager la charge.

unit parallel-join *num_of_units* **max-bundle-delay** *max_delay_time*

- *num_of_units* : spécifie le nombre minimum de modules dans le même châssis qui doivent être prêts avant qu'un module puisse rejoindre la grappe (entre 1 et 3). La valeur par défaut est 1, ce qui signifie qu'un module n'attendra pas que les autres modules soient prêts avant de rejoindre la grappe. Par exemple, si vous définissez la valeur à 3, chaque module attendra *max_delay_time* ou jusqu'à ce que les trois modules soient prêts avant de rejoindre la grappe. Les trois modules demanderont de rejoindre la grappe presque simultanément et commenceront tous à recevoir du trafic à peu près au même moment.
- *max_delay_time* : spécifie le délai maximum en minutes avant qu'un module arrête d'attendre que d'autres modules soient prêts avant de rejoindre la grappe, entre 0 et 30 minutes. La valeur par défaut est 0, ce qui signifie que le module n'attendra pas que les autres modules soient prêts avant de rejoindre la grappe. Si vous définissez le *num_of_units* sur 1, cette valeur doit être de 0. Si vous définissez le *num_of_units* sur 2 ou 3, cette valeur doit être de 1 ou plus. Cette minuterie est définie par module, mais lorsque le premier module rejoint la grappe, toutes les autres minuteries du module se terminent et les modules restants rejoignent la grappe.

Par exemple, vous définissez le *num_of_units* sur 3 et le *max_delay_time* sur 5 minutes. Lorsque le module 1 apparaît, il démarre sa minuterie de 5 minutes. Le module 2 apparaît 2 minutes plus tard et démarre sa minuterie de 5 minutes. Le module 3 apparaît 1 minute plus tard. Par conséquent, tous les modules rejoindront désormais la grappe au bout de 4 minutes; ils n'attendront pas la fin de la minuterie. Si le module 3 n'apparaît jamais, le module 1 rejoindra la grappe à la fin de sa minuterie de 5 minutes et le module 2 rejoindra également la grappe, même s'il reste 2 minutes à s'écouler; il n'attendra pas la fin de sa minuterie.

Étape 7 Configurez le nombre maximum de membres de la grappe.

cluster-member-limit *number*

- *number* : de 2 à 16. Par défaut, c'est 16.

Si vous savez que votre grappe sera inférieure au maximum de 16 unités, nous vous conseillons de définir le nombre d'unités réel planifié. La définition du nombre maximum d'unités permet à la grappe de mieux gérer les ressources. Par exemple, si vous utilisez la traduction d'adresse de port (PAT), l'unité de contrôle peut ensuite allouer des blocs de ports au nombre de membres planifié sans avoir à réserver des ports pour des unités supplémentaires que vous ne comptez pas utiliser.

Configurer les paramètres de surveillance de l'intégrité et de jonction automatique

Cette procédure permet de configurer la surveillance de l'intégrité des unités et des interfaces.

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. Vous pouvez superviser n'importe quel ID de canal de port ou ID d'interface physique unique. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles

telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Étape 2 Personnalisez la fonctionnalité de contrôle de l'intégrité des unités de la grappe :

health-check [**holdtime** *timeout*]

La commande **holdime** détermine l'intervalle de temps entre les messages d'état heartbeat des unités, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes.

Pour déterminer l'intégrité des unités, les unités de grappe ASA envoient à d'autres unités des messages de signal de présence heartbeat sur la liaison de commande de grappe. Si une unité ne reçoit aucun message heartbeat d'une unité homologue pendant la période d'attente, l'unité homologue est considérée comme ne répondant pas ou morte.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA, le Châssis Firepower 4100/9300 ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise, ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées (**no health-check monitor-interface**). Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.

Exemple :

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

Étape 3 Désactivez le contrôle d'intégrité de l'interface sur une interface :

no health-check monitor-interface [*interface_id* | **service-application**]

La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur une unité particulière, mais qu'il y a des ports actifs sous la même interface logique sur d'autres unités, l'unité est supprimée de la grappe. Le délai avant que l'ASA ne supprime un membre de la grappe dépend du type d'interface et du fait que l'unité soit un membre établi ou en voie de se joindre à la grappe.

Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces. Vous pouvez le désactiver pour chaque interface en utilisant la forme **no** de cette commande. Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée. Spécifiez le **service-application** pour désactiver la surveillance d'une application décoratrice.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA, le Châssis Firepower 4100/9300 ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise, ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité (**no health-check**) et désactiver la surveillance d'interface

pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.

Exemple :

```
ciscoasa(cfg-cluster)# no health-check monitor-interface port-channel1
```

Étape 4 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité :

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system** : spécifie les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.
- **unlimited** : (Par défaut pour le **cluster-interface**) Ne limite pas le nombre de tentatives de jonction.
- *auto-rejoin-max* : définit le nombre de tentatives de jonction, entre 0 et 65535. **0** désactive la jonction automatique. La valeur par défaut pour les commandes **data-interface** et **system** est de 3.
- *auto_rejoin_interval* : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. La durée totale maximale pendant laquelle l'unité tente de rejoindre la grappe est limitée à 14400 minutes (10 jours) à compter du dernier échec.
- *auto_rejoin_interval_variation* : définit si la durée de l'intervalle augmente. Définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données et le système

Exemple :

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

Étape 5 Configurez le délai antirebond avant que l'ASA considère une interface comme défaillante et que l'unité ne soit supprimée de la grappe.

health-check monitor-interface debounce-time *ms*

Définissez le délai antirebond entre 300 et 9 000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme défaillante, et l'unité est supprimée de la grappe. Par exemple, dans le cas d'un EtherChannel qui passe d'un état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un délai de réponse plus long peut empêcher l'interface de sembler être défaillante sur une unité de la grappe juste parce qu'une autre unité de la grappe a été plus rapide à regrouper les ports.

Exemple :

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

Étape 6 Configurez l'intervalle de vérification de l'intégrité du châssis :

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

- **interval** *ms* : définissez la durée entre les pulsations, entre 100 et 6 000 ms, en multiples de 100. La valeur par défaut est 1000ms.
- **retry-count** *number* : définissez le nombre de tentatives, entre 1 et 30. La valeur par défaut est de 3 tentatives.

L'ASA vérifie s'il peut communiquer via le fond de panier avec le châssis hôte.

La durée minimum combinée (*intervalle* x *nombre de tentatives*) ne peut pas être inférieure à 600 ms. Par exemple, si vous définissez l'intervalle sur 100 et le nombre de nouvelles tentatives sur 3, la durée totale combinée est de 300 ms, ce qui n'est pas pris en charge. Par exemple, vous pouvez définir l'intervalle sur 100 et le nombre de nouvelles tentatives sur 6 pour respecter la durée minimum (600 ms).

Exemple :

```
ciscoasa(cfg-cluster)# app-agent heartbeat interval 1000 retry-count 10
```

Étape 7 (Facultatif) Configurez la surveillance de la charge de trafic.

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* : définit le délai en secondes entre les messages de surveillance, entre 10 et 360 secondes. La valeur par défaut est de 20 secondes.
- **intervals** *intervals* : définit le nombre d'intervalles pour lesquels l'ASA conserve les données, entre 1 et 60. La valeur par défaut est 30.

Vous pouvez superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur l'unité si les unités restantes peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Par exemple, pour la mise en grappe inter-châssis sur le Firepower 9300 avec 3 modules de sécurité dans chaque châssis, si deux modules de sécurité d'un châssis quittent la grappe, la même quantité de trafic vers le châssis sera envoyée au module restant et risque de le submerger. Vous pouvez superviser périodiquement la charge de trafic. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur l'unité.

Utilisez la commande **show cluster info load-monitor** pour afficher la charge de trafic.

Exemple :

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
```

```
1           0           0           13              27
```

Configurer la rééquilibrage de la connexion et le délai de réplication TCP de la grappe

Vous pouvez configurer le rééquilibrage des connexions. Vous pouvez activer le délai de réplication de grappe pour les connexions TCP pour aider à éliminer le « travail inutile » lié aux flux de courte durée en retardant la création du flux directeur/de sauvegarde. Notez que si une unité tombe en panne avant la création du flux directeur/de sauvegarde, ces flux ne peuvent pas être récupérés. De même, si le trafic est rééquilibré vers une autre unité avant la création du flux, le flux ne peut pas être récupéré. Vous ne devez pas activer la réplication TCP pour le trafic sur lequel vous désactivez la répartition aléatoire TCP.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Étape 2 (Facultatif) Activez le rééquilibrage des connexions pour le trafic TCP :

conn-rebalance [**frequency** *seconds*]

Exemple :

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

Cette commande est désactivée par défaut. Si cette option est activée, les ASA échangent périodiquement des renseignements sur les connexions par seconde et déchargent les nouvelles connexions des appareils ayant plus de connexions par seconde vers les appareils moins chargés. Les connexions existantes ne sont jamais déplacées. De plus, comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées. La valeur par défaut est de 5 secondes.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Étape 3 Activez le délai de réplication de la grappe pour les connexions TCP :

cluster replication delay *seconds* {**http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] {**host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

Exemple :

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

Définissez les *secondes* entre 1 et 15. Le délai **http** est activé par défaut pendant 5 secondes.

Configurer les fonctionnalités inter-sites

Pour la mise en grappe inter-sites, vous pouvez personnaliser votre configuration pour améliorer la redondance et la stabilité.

Activer la localisation du directeur

Pour améliorer les performances et réduire la latence d'aller-retour dans le cas de la mise en grappe inter-sites pour les centres de données, vous pouvez activer la localisation du directeur. Les nouvelles connexions sont généralement équilibrées et appartiennent aux membres de la grappe d'un site donné. Cependant, l'ASA attribue le rôle de directeur à un membre sur *n'importe quel* site. La localisation du directeur permet des rôles de directeur supplémentaires : un directeur local sur le même site que le propriétaire et un directeur global qui peut se trouver sur n'importe quel site. Le fait de maintenir le propriétaire et le directeur sur le même site améliore les performances. En cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site. Le directeur global est utilisé si un membre d'une grappe reçoit des paquets pour une connexion appartenant à un autre site.

Avant de commencer

- Définissez l'ID de site du châssis sur le superviseur Châssis Firepower 4100/9300 .
- Les types de trafic suivants ne prennent pas en charge la localisation : trafic NAT ou PAT; trafic inspecté par SCTP; requête du propriétaire de la fragmentation.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

Étape 2 Activez la localisation du directeur :

director-localization

Activer la redondance de site

Pour protéger les flux contre une défaillance de site, vous pouvez activer la redondance de site. Si le propriétaire de connexion de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site.

Avant de commencer

- Définissez l'ID de site du châssis sur le superviseur Châssis Firepower 4100/9300 .

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

Étape 2 Activez la redondance de site.

site-redundancy

Configurer l'ARP gratuit par site

L'ASA génère des paquets ARP gratuits (GARP) pour maintenir l'infrastructure de commutation à jour : le membre ayant la priorité la plus élevée sur chaque site génère périodiquement du trafic GARP pour les adresses MAC et IP globales.

Lorsque vous utilisez des adresses MAC et IP par site, les paquets provant de la grappe utilisent une adresse MAC et une adresse IP propres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IP globales. Si le trafic n'est pas généré périodiquement à partir de l'adresse MAC globale, vous pourriez rencontrer un délai d'expiration de l'adresse MAC sur vos commutateurs pour l'adresse MAC globale. Après un délai d'expiration, le trafic destiné à l'adresse MAC globale sera inondé dans l'ensemble de l'infrastructure de commutation, ce qui peut entraîner des problèmes de performance et de sécurité.

Le GARP est activé par défaut lorsque vous définissez l'ID de site pour chaque unité et l'adresse MAC du site pour chaque EtherChannel étendu. Vous pouvez personnaliser l'intervalle GARP ou vous pouvez désactiver GARP.

Avant de commencer

- Définissez l'ID de site pour le membre de la grappe dans la configuration de démarrage.
- Définissez l' adresse MAC par site pour l' EtherChannel étendu dans la configuration de l'unité de contrôle.

Procédure

Étape 1 Entrez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group cluster1
```

```
ciscoasa(cfg-cluster)#
```

Étape 2 Personnalisez l'intervalle GARP.

site-periodic-garp interval *seconds*

- *seconds* :Définissez le temps en secondes entre la génération du GARP, entre 1 et 1000000 secondes. La valeur par défaut est de 290 secondes.

Pour désactiver GARP, saisissez **no site-periodic-garp interval**.

Exemple :

```
ciscoasa(cfg-cluster)# site-periodic-garp interval 500
```

Configurer la mobilité des flux de grappes

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

À propos de l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux entre les sites.

À propos de LISP

La mobilité des machines virtuelles de centres de données, comme VMware VMotion, permet aux serveurs de migrer entre les centres de données tout en maintenant les connexions avec les clients. Pour prendre en charge une telle mobilité de serveur de centre de données, les routeurs doivent être en mesure de mettre à jour la route d'entrée vers le serveur lorsqu'il se déplace. L'architecture Cisco Locator/Protocole de séparation d'ID (LISP) sépare l'identité du périphérique, ou l'identifiant de terminal (EID), de son emplacement, ou localisateur de routage, dans deux espaces de numérotation différents, ce qui rend la migration du serveur transparente pour les clients. Par exemple, lorsqu'un serveur est déplacé vers un nouveau site et qu'un client envoie du trafic vers le serveur, le routeur redirige le trafic vers le nouvel emplacement.

LISP nécessite des routeurs et des serveurs dans certains rôles, tels que le routeur de tunnel de sortie (ETR) LISP, le routeur de tunnel d'entrée (ITR), les routeurs de premier saut, le résolveur de carte (MR) et le serveur de carte (MS). Lorsque le routeur du premier saut du serveur détecte que le serveur est connecté à un autre routeur, il met à jour tous les autres routeurs et les bases de données afin que l'ITR connectée au client puisse intercepter, encapsuler et envoyer le trafic vers le nouvel emplacement du serveur.

Prise en charge du LISP Cisco Secure Firewall ASA

L'ASA n'exécute pas le LISP lui-même; il peut, cependant, inspecter le trafic LISP pour détecter les changements d'emplacement, puis utiliser ces informations pour un fonctionnement de mise en grappe transparent. Sans l'intégration du LISP, lorsqu'un serveur est déplacé vers un nouveau site, le trafic est acheminé vers un membre de la grappe ASA sur le nouveau site plutôt que vers le propriétaire d'origine du flux. Le nouvel ASA transfère le trafic vers l'ASA au niveau de l'ancien site, puis l'ancien ASA doit renvoyer le trafic vers le nouveau site pour qu'il atteigne le serveur. Ce flux de trafic est sous-optimal et est connu comme « tromboning » ou « épingle à cheveux ».

Grâce à l'intégration du LISP, les membres de la grappe ASA peuvent inspecter le trafic LISP passant entre le routeur du premier saut et l'ETR ou l'ITR, puis peuvent changer le propriétaire du flux pour qu'il se trouve sur le nouveau site.

Lignes directrices LISP

- Les membres de la grappe ASA doivent se trouver entre le routeur du premier saut et l'ITR ou l'ETR du site. La grappe ASA elle-même ne peut pas être le premier routeur de saut pour un segment étendu.
- Seuls les flux entièrement distribués sont pris en charge; les flux centralisés, les flux semi-distribués ou les flux appartenant à des nœuds individuels ne sont pas transférés vers de nouveaux propriétaires. Les flux semi-distribués comprennent des applications, telles que SIP, où tous les flux enfants appartiennent au même ASA qui possède le flux parent.
- La grappe déplace uniquement les états de flux de couche 3 et 4; certaines données d'application pourraient être perdues.
- Pour les flux de courte durée ou non essentiels pour l'entreprise, le déplacement du propriétaire peut ne pas valoir la peine. Vous pouvez contrôler les types de trafic pris en charge avec cette fonctionnalité lorsque vous configurez la politique d'inspection. Vous devez limiter la mobilité de flux au trafic essentiel.

Mise en œuvre du LISP ASA

Cette fonctionnalité comprend plusieurs configurations interdépendantes (qui sont toutes décrites dans ce chapitre) :

1. (Facultatif) Limiter les EID inspectés en fonction de l'adresse IP de l'hôte ou du serveur : le routeur de premier saut pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée, vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.
2. Inspection du trafic LISP : l'ASA inspecte le trafic LISP sur le port UDP 4342 pour détecter le message EID-notify envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui met en corrélation l'EID et l'ID de site. Par exemple, vous devez inspecter le trafic LISP avec une adresse IP source du routeur du premier saut et une adresse de destination de l'ITR ou de l'ETR. Remarque : le trafic LISP n'a pas de directeur affecté et le trafic LISP en lui-même ne participe pas au partage de l'état de la grappe.
3. Politique de service pour activer la mobilité des flux sur le trafic spécifié : vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.
4. ID de sites : l'ASA utilise l'ID de site pour chaque nœud de la grappe afin de déterminer le nouveau propriétaire.
5. Configuration au niveau de la grappe pour activer la mobilité de flux : vous devez également activer la mobilité de flux au niveau de la grappe. Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité de flux pour une classe particulière de trafic ou d'applications.

Configurer l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

Avant de commencer

- Définissez l'ID de site du châssis sur le superviseur Châssis Firepower 4100/9300 .

- Le trafic LISP n'est pas inclus dans la classe de trafic d'inspection par défaut. Vous devez donc configurer une classe distincte pour le trafic LISP dans le cadre de cette procédure.

Procédure

Étape 1 (Facultatif) Configurez une carte d'inspection LISP pour limiter les EID inspectés en fonction de l'adresse IP et pour configurer la clé partagée LISP :

a) Créez une ACL étendue; seule l'adresse IP de destination correspond à l'adresse intégrée de l'EID :

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

Les ACL IPv4 et IPv6 sont acceptées. Consultez la référence de commande pour connaître la syntaxe **access-list extended** exacte.

b) Créez la carte d'inspection LISP et entrez le mode des paramètres :

policy-map type inspect lisp *inspect_map_name*

parameters

c) Définissez les EID autorisés en identifiant l'ACL que vous avez créée :

allowed-eid access-list *eid_acl_name*

Le routeur de premier saut ou l'ITR/ETR pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée; vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.

d) Si nécessaire, saisissez la clé partagée :

validate-key *key*

Exemple :

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

Étape 2 Configurez l'inspection LISP pour le trafic UDP entre le routeur de premier saut et l'ITR ou l'ETR sur le port 4342 :

a) Configurez l'ACL étendue pour identifier le trafic LISP :

access list *inspect_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

Vous *devez* spécifier le port UDP 4342. Les ACL IPv4 et IPv6 sont acceptées. Consultez la référence de commande pour connaître la syntaxe **access-list extended** exacte.

b) Créez une carte de trafic pour l'ACL :

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) Spécifiez la liste des politiques, la carte de trafic, activez l'inspection à l'aide de la carte d'inspection LISP facultative et appliquez la politique de service à une interface (si nouvelle) :

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

Si vous avez une politique de service existante, spécifiez le nom de la liste des politiques existante. Par défaut, l'ASA inlcut une politique globale appelée **global_policy**, donc pour une politique globale, spécifiez ce nom. Vous pouvez également créer une politique de service par interface si vous ne souhaitez pas appliquer la politique à l'échelle mondiale. L'inspection LISP est appliquée au trafic de manière bidirectionnelle, vous n'avez donc pas besoin d'appliquer la politique de service sur les interfaces source et de destination; tout le trafic qui entre ou sort de l'interface à laquelle vous appliquez la liste des politiques est affecté si le trafic correspond à la carte de trafic dans les deux sens.

Exemple :

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

L'ASA inspecte le trafic LISP pour détecter le message de notification d'EID envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui met en corrélation l'EID et l'ID de site.

Étape 3 Activez la mobilité des flux pour une classe de trafic :

a) Configurez l'ACL étendue pour identifier le trafic opérationnel critique que vous souhaitez réaffecter au site le plus optimal lorsque les serveurs changent de site :

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

Les ACL IPv4 et IPv6 sont acceptées. Consultez la référence de commande pour connaître la syntaxe **access-list extended** exacte. Vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.

b) Créez une carte de trafic pour l'ACL :

class-map *flow_map_name*

match access-list *flow_acl_name*

c) Spécifiez la même liste des politiques sur laquelle vous avez activé l'inspection LISP, la carte de trafic de flux, et activez la mobilité des flux :

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

Exemple :

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

Étape 4 Entrez dans le mode de configuration du groupe de grappes et activez la mobilité des flux pour la grappe :

cluster group *name*

flow-mobility lisp

Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité des flux.

Exemples

L'exemple suivant :

- Limite les EID à ceux sur le réseau 10.10.10.0/24
- Inspecte le trafic LISP (UDP 4342) entre un routeur LISP à l'adresse 192.168.50.89 (à l'intérieur) et un routeur ITR ou ETTR (sur une autre interface ASA) à l'adresse 192.168.10.8
- Active la mobilité des flux pour tout le trafic interne vers un serveur sur 10.10.10.0/24 à l'aide de HTTPS.
- Active la mobilité des flux pour la grappe.

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

Configurer le VPN de site à site distribué

Par défaut, la grappe utilise le mode VPN de site à site centralisé. Pour profiter de l'évolutivité de la mise en grappe, vous pouvez activer le mode VPN de site à site distribué.

À propos du VPN de site à site distribué

En mode distribué, les connexions VPN IPsec IKEv2 de site à site sont réparties sur les nœuds d'une grappe. La distribution des connexions VPN sur les nœuds d'une grappe permet d'utiliser pleinement la capacité et le débit de la grappe, ce qui augmente considérablement la prise en charge des VPN au-delà des capacités VPN centralisées.

Rôles de connexion du VPN distribué

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée. Lors de l'exécution en mode VPN distribué, les rôles suivants sont affectés aux nœuds de la grappe :

- Propriétaire de session active : le nœud qui reçoit initialement la connexion ou qui a effectué la transition d'une session de sauvegarde en une session active. Le propriétaire conserve l'état et traite les paquets pour toute la session, y compris les tunnels IKE et IPsec et tout le trafic qui leur est associé.
- Propriétaire de la session de sauvegarde : le nœud qui gère la session de sauvegarde pour une session active existante. En cas d'échec du propriétaire de la session active, le propriétaire de la session de secours devient le propriétaire de la session active et une nouvelle session de sauvegarde est établie sur un autre nœud.
- Transmetteur : si le trafic associé à une session VPN est envoyé à un nœud qui n'est pas propriétaire de la session VPN, ce nœud utilisera la liaison de commande de grappe pour transmettre le trafic au nœud propriétaire de la session VPN.
- Orchestrateur : l'orchestrateur (toujours le nœud de contrôle de la grappe) est responsable du calcul des sessions qui se déplaceront et de la destination lors de l'exécution d'une redistribution de sessions actives (ASR). Il envoie une demande au nœud propriétaire X de déplacer N sessions vers le nœud Y. Le nœud X répondra à l'orchestrateur une fois terminé, en précisant le nombre de sessions qu'il a pu déplacer.

Caractéristiques de session du VPN distribué

Les sessions VPN de site à site distribuées présentent les caractéristiques suivantes. Sinon, les connexions VPN se comportent normalement, comme si elles n'étaient pas sur une grappe.

- Les sessions VPN sont réparties dans la grappe au niveau de la session. Cela signifie que le même nœud de grappe gère les tunnels IKE et IPsec et tout leur trafic pour une connexion VPN. Si le trafic de session VPN est envoyé à un nœud de grappe qui ne possède pas cette session VPN, le trafic est transféré au nœud de grappe qui est propriétaire de la session VPN.
- Les sessions VPN ont un ID de session unique dans la grappe. À l'aide de l'ID de session, le trafic est validé, des décisions de transfert sont prises et la négociation IKE est terminée.
- Dans une configuration en étoile avec un VPN de site à site, lorsque les clients se connectent au moyen de la grappe (ce que l'on appelle le hair-pinning), le trafic de session entrant et le trafic de session sortant peuvent se trouver sur des nœuds de grappe différents.
- Vous pouvez exiger que la session de sauvegarde soit allouée sur un module de sécurité dans un autre châssis; cela offre une protection contre les défaillances de châssis. Vous pouvez également choisir

d'allouer des sessions de sauvegarde sur n'importe quel nœud de la grappe; cela offre une protection uniquement contre les défaillances de nœuds. Lorsque la grappe contient deux châssis, la sauvegarde sur le châssis distant est fortement conseillée.

Gestion des événements de grappe par le VPN distribué

Événement	VPN distribué
Défaillance de nœud	Pour toutes les sessions actives sur ce nœud défaillant, les sessions de sauvegarde (sur un autre nœud) deviennent actives et les sessions de sauvegarde sont réaffectées sur un autre nœud en fonction de la stratégie de sauvegarde.
Défaillance du châssis	Lorsqu'une stratégie de sauvegarde de châssis distant est utilisée, pour toutes les sessions actives sur le châssis défaillant, les sessions de sauvegarde (sur un nœud de l'autre châssis) deviennent actives. Lorsque les nœuds seront remplacés, les sessions de sauvegarde pour ces sessions désormais actives seront réaffectées sur les nœuds du châssis remplacé. Lorsqu'une stratégie de sauvegarde plate est utilisée, si les sessions actives et de sauvegarde se trouvent sur le châssis défaillant, la connexion sera abandonnée. Toutes les sessions actives avec des sessions de sauvegarde sur un nœud de l'autre châssis reviennent à ces sessions. De nouvelles sessions de sauvegarde seront attribuées sur un autre nœud du châssis restant.
Désactiver un nœud de grappe	Pour toutes les sessions actives sur le nœud de grappe qui sont désactivées, les sessions de sauvegarde (sur un autre nœud) deviennent actives et réaffectent les sessions de sauvegarde sur un autre nœud en fonction de la stratégie de sauvegarde.
Joindre un nœud de grappe	Si le mode de grappe VPN sur le nouveau nœud n'est pas distribué, le nœud de contrôle demandera un changement de mode. Une fois que le mode VPN est compatible, le nœud de la grappe se verra attribuer des sessions actives et de sauvegarde dans le flux des opérations normales.

Modifications IPsec IKEv2

IKEv2 est modifié en mode VPN de site à site distribué de la manière suivante :

- Une identité est utilisée à la place des tuples IP/port. Cela permet de prendre des décisions de transfert appropriées sur les paquets et de nettoyer les connexions précédentes qui peuvent se trouver sur d'autres membres de la grappe.
- Les identifiants (SPI) qui identifient une seule session IKEv2 sont des valeurs aléatoires de 8 octets générées localement et uniques dans toute la grappe. Un SPI intègre un horodatage et un ID de nœud de grappe. À la réception d'un paquet de négociation IKE, si la vérification de l'horodatage ou de l'ID du nœud de la grappe échoue, le paquet est abandonné et un message est enregistré pour indiquer la raison.
- Le traitement IKEv2 a été modifié pour empêcher les négociations NAT-T d'échouer en étant réparties entre les membres de la grappe. Un nouveau domaine de classification ASP, *cluster_isakmp_redirect*, et des règles sont ajoutés lorsque IKEv2 est activé sur une interface. Utilisez la commande **show asp table classify domain cluster_isakmp_redirect** pour afficher les règles.

Haute disponibilité pour le VPN de site à site distribué dans la grappe

Les fonctionnalités suivantes offrent une résilience contre la défaillance unique d'un module ou d'un châssis de sécurité :

- Les sessions VPN qui sont sauvegardées sur un autre module de sécurité de la grappe, sur n'importe quel châssis, supportent les défaillances de module de sécurité.
- Les sessions VPN sauvegardées sur un autre châssis supportent les défaillances de châssis.
- Le nœud de contrôle peut changer sans perdre les sessions VPN de site à site.

Si une défaillance supplémentaire se produit avant que la grappe ne soit stable, les connexions peuvent être perdues si les sessions actives et de secours se trouvent sur les nœuds défaillants.

Toutes les tentatives sont faites pour assurer qu'aucune session ne soit perdue lorsqu'un nœud quitte la grappe de manière progressive, comme la désactivation du mode grappe VPN, le rechargement d'un nœud de grappe et d'autres modifications de châssis anticipées. Pendant ce type d'opérations, les sessions ne seront pas perdues tant que la grappe aura le temps de rétablir les sauvegardes de sessions entre les opérations. Si une sortie progressive est déclenchée sur le dernier nœud de la grappe, elle supprimera rapidement les sessions existantes.

CMPv2

Le certificat d'identification et les paires de clés CMPv2 sont synchronisés sur les nœuds de la grappe. Cependant, seul le nœud de contrôle de la grappe renouvelle automatiquement et resaisit le certificat CMPv2. Le nœud de contrôle synchronise ces nouveaux certificats d'identification et clés avec tous les nœuds de la grappe lors d'un renouvellement. De cette façon, tous les nœuds de la grappe utilisent les certificats CMPv2 pour l'authentification, et tous les nœuds sont capables de prendre le relais en tant que nœud de contrôle.

Licences pour le VPN de site à site distribué

Une licence d'opérateur est requise pour le VPN de site à site distribué, sur chaque membre de la grappe.

Chaque connexion VPN nécessite deux sessions sous licence *Other VPN* (Autre VPN) (la licence *Other VPN* (Autre VPN) fait partie de la licence *Essentials*), une pour la session active et une pour la session de secours. La capacité maximale de sessions VPN de la grappe ne peut pas dépasser la moitié de la capacité sous licence en raison de l'utilisation de deux licences pour chaque session.

Conditions préalables au VPN de site à site distribué

Prise en charge des modèles

- Firepower 9300
- Maximum de 6 modules sur 2 châssis. Vous pouvez installer un nombre différent de modules de sécurité dans chaque châssis, mais nous conseillons une répartition égale.

Maximum de sessions VPN

Chaque module de sécurité prend en charge jusqu'à 6 000 sessions VPN pour un maximum d'environ 36 000 sessions sur 6 nœuds.

Le nombre réel de sessions prises en charge sur un nœud de grappe est déterminé par la capacité de la plateforme, les licences allouées et l'allocation des ressources par contexte. Lorsque l'utilisation est proche de la limite, il peut arriver que la création de sessions échoue, même si la capacité maximum n'a pas été atteinte sur chaque nœud de la grappe. En effet, l'allocation de sessions actives est déterminée par une

commutation externe et l'allocation de sessions de secours est déterminée par un algorithme de grappe interne. Nous invitons les clients à dimensionner leur utilisation en conséquence et à prévoir une marge pour une répartition inégale.

Lignes directrices relatives au VPN de site à site distribué

Mode pare-feu

Le VPN de site à site distribué est pris en charge en mode routé uniquement.

Mode contextuel

Le VPN de site à site distribué fonctionne à la fois en mode de contexte unique et en mode de contexte multiple. Cependant, en mode de contexte multiple, la redistribution des sessions actives est effectuée au niveau du système, et non au niveau du contexte. Cela empêche une session active associée à un contexte de se déplacer vers un membre de grappe qui contient des sessions actives associées à un contexte différent, créant ainsi une charge non pris en charge.

Inspections non prises en charge

Les types d'inspections suivants ne sont pas pris en charge ou sont désactivés en mode VPN de site à site distribué :

- CTIQBE
- DCERPC
- H323, H225 et RAS
- Intercommunication IPsec
- MGCP
- MMP
- NetBIOS
- PPTP
- RADIUS
- RSH
- RTSP
- SCCP (Skinny)
- SunRPC
- TFTP
- WAAS
- WCCP
- XDMCP

Directives supplémentaires

- Seul le VPN de site à site IKEv2 IPsec est pris en charge en mode VPN de site à site distribué. IKEv1 n'est pas pris en charge. Le VPN de site à site IKEv1 est pris en charge en mode VPN centralisé.
- La mise en grappe inter-sites n'est pas prise en charge.
- La PAT dynamique n'est pas disponible en mode VPN de site à site distribué.

Activer le VPN de site à site distribué

Activez le VPN de site à site distribué pour profiter de l'évolutivité de la mise en grappe pour les sessions VPN.



Remarque Le passage du mode VPN entre centralisé et distribué nécessite le rechargement de tous les nœuds de la grappe. La modification du mode de sauvegarde est dynamique et ne mettra pas fin aux sessions.

Avant de commencer

Configurez le VPN de site à site en fonction du guide de configuration de VPN.

Procédure

Étape 1 Sur le nœud de contrôle de la grappe, passez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

Étape 2 Activez le VPN de site à site distribué.

vpn-mode distributed backup flat

ou

vpn-mode distributed backup remote-chassis

En mode de sauvegarde **plate**, des sessions de veille sont établies sur n'importe quel autre nœud de la grappe. Cela protégera les utilisateurs contre les défaillances de module; cependant, la protection contre les défaillances de châssis n'est pas garantie.

En mode de sauvegarde du **châssis distant**, des sessions de veille sont établies sur un nœud d'un autre châssis de la grappe. Cela protégera les utilisateurs contre les défaillances de module et de châssis.

Si le **châssis distant** est configuré dans un environnement de châssis unique (configuré intentionnellement ou à la suite d'une défaillance), aucune sauvegarde ne sera créée avant qu'un autre châssis rejoigne la grappe.

Exemple :

```
ciscoasa(cfg-cluster)# vpn-mode distributed backup remote-chassis
```

```
WARNING: Do you want to proceed with changing the vpn-mode, save the device configuration,
and initiate a reboot? [confirm]
```

Redistribuer les sessions du VPN S2S distribué

La redistribution des sessions actives redistribue la charge des sessions VPN actives sur les nœuds de la grappe. En raison de la nature dynamique des sessions de début et de fin, la redistribution des sessions actives permet d'équilibrer au mieux les sessions sur tous les nœuds de la grappe. Des actions de redistribution répétées optimiseront l'équilibre.

La redistribution peut être exécutée à tout moment, mais il est conseillé de la réaliser après toute modification de topologie dans la grappe et après qu'un nouveau nœud a rejoint la grappe. L'objectif de la redistribution est de créer une grappe VPN stable. Une grappe VPN stable a un nombre presque égal de sessions actives et de sauvegarde sur les nœuds.

Pour déplacer une session, la session de sauvegarde devient active et un autre nœud est sélectionné pour héberger une nouvelle session de sauvegarde. Le déplacement des sessions dépend de l'emplacement de la sauvegarde de la session active et du nombre de sessions actives déjà sur ce nœud de sauvegarde en particulier. Si le nœud de session de sauvegarde ne peut pas héberger la session active pour une raison quelconque, le nœud d'origine reste propriétaire de la session.

En mode de contexte multiple, la redistribution des sessions actives est effectuée au niveau du système, et non au niveau du contexte individuel. Elle ne se fait pas au niveau du contexte, car une session active dans un contexte peut déplacer un nœud qui contient de nombreuses sessions actives dans un contexte différent, créant ainsi une charge plus importante sur ce nœud de grappe.

Avant de commencer

- Activez les journaux système si vous souhaitez superviser l'activité de redistribution.
- Cette procédure doit être effectuée sur l'unité de contrôle de la grappe.

Procédure

Étape 1 Sur le nœud de contrôle, affichez la répartition des sessions actives et de sauvegarde dans la grappe.

show cluster vpn-sessiondb distribution

Exemple :

Les renseignements sur la distribution s'affichent comme suit :

```
ciscoasa# show cluster vpn-sessiondb distribution
Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)
Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)
Member 2 (unit-1-2): active: 0
```

Chaque ligne contient l'ID du membre, le nom du membre, le nombre de sessions actives et les membres sur lesquels se trouvent les sessions de sauvegarde. Dans l'exemple ci-dessus, on lit les renseignements comme suit :

- Le membre 0 a 209 sessions actives, 111 sessions sont sauvegardées sur le membre 1, 98 sessions sont sauvegardées sur le membre 2
- Le membre 1 a 204 sessions actives, 108 sessions sont sauvegardées sur le membre 0, 96 sessions sont sauvegardées sur le membre 2
- Le membre 2 n'a AUCUNE session active; par conséquent, aucun membre de la grappe ne sauvegarde de sessions pour ce nœud. Ce membre a récemment rejoint la grappe.

Étape 2 Redistribuez les sessions.

cluster redistribute vpn-sessiondb

Cette commande se termine immédiatement (sans message) pendant qu'elle s'exécute en arrière-plan.

Selon le nombre de sessions à redistribuer et la charge sur la grappe, cela peut prendre un certain temps. Les journaux système contenant les expressions suivantes (et d'autres détails sur le système non affichés ici) sont fournis au fur et à mesure que l'activité de redistribution se produit :

Expression du journal système	Notes
Redistribution de la session VPN démarrée	Nœud de contrôle uniquement
Demande envoyée pour déplacer *nombre* sessions de *orig-member-name* à *dest-member-name*	Nœud de contrôle uniquement
Échec de l'envoi du message de redistribution de session à *member-name*	Nœud de contrôle uniquement
Demande reçue pour déplacer *nombre* sessions de *orig-member-name* à *dest-member-name*	Nœud de données uniquement
Déplacement de *nombre* sessions à *member-name*	Le nombre de sessions actives déplacées vers la grappe nommée.
Échec de la réception de la réponse de déplacement de session depuis *dest-member-name*	Nœud de contrôle uniquement
Session VPN terminée	Nœud de contrôle uniquement
Modification de la topologie de grappe détectée. Redistribution de la session VPN abandonnée.	

Étape 3 Saisissez à nouveau la commande **show cluster vpn-sessiondb distribution** pour afficher les résultats.

FXOS : supprimer un nœud de la grappe

Les sections suivantes décrivent comment supprimer des nœuds de façon temporaire ou permanente de la grappe.

Suppression temporaire

Un nœud de grappe sera automatiquement supprimé de la grappe en raison d'une défaillance matérielle ou réseau, par exemple. Cette suppression est temporaire jusqu'à ce que les conditions soient rectifiées, et qu'il puisse rejoindre la grappe. Vous pouvez également désactiver manuellement la mise en grappe.

Pour vérifier si un appareil se trouve actuellement dans la grappe, vérifiez l'état de la grappe de l'application à l'aide de la commande **show cluster info** : :

```
ciscoasa# show cluster info
Clustering is not enabled
```

- Disable clustering in the application (désactivez la mise en grappe dans l'application) : Vous pouvez désactiver la mise en grappe à l'aide de l'interface de ligne de commande de l'application. Saisissez la commande **cluster remove unit** *name* pour supprimer tout nœud autre que celui auquel vous êtes connecté. La configuration de démarrage reste inchangée, ainsi que la dernière configuration synchronisée à partir du nœud de contrôle, afin que vous puissiez rajouter le nœud ultérieurement sans perdre votre configuration. Si vous saisissez cette commande sur un nœud de données pour supprimer le nœud de contrôle, un nouveau nœud de contrôle est élu.

  Lorsqu'un périphérique devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de la configuration de démarrage. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée.

  Pour réactiver la mise en grappe, saisissez le **cluster group** *name* sur l'ASA, puis **enable**.

- Désactivez l'instance d'application : Au niveau de l'interface de ligne de commande de FXOS, voyez l'exemple suivant :

  ```
  Firepower-chassis# scope ssa
  Firepower-chassis /ssa # scope slot 1
  Firepower-chassis /ssa/slot # scope app-instance asa asa1
  Firepower-chassis /ssa/slot/app-instance # disable
  Firepower-chassis /ssa/slot/app-instance* # commit-buffer
  Firepower-chassis /ssa/slot/app-instance #
  ```

  Pour réactiver :

  ```
  Firepower-chassis /ssa/slot/app-instance # enable
  Firepower-chassis /ssa/slot/app-instance* # commit-buffer
  Firepower-chassis /ssa/slot/app-instance #
  ```

- Arrêtez le security module/engine : Au niveau de l'interface de ligne de commande de FXOS, voyez l'exemple suivant :

  ```
  Firepower-chassis# scope service-profile server 1/1
  Firepower-chassis /org/service-profile # power down soft-shut-down
  Firepower-chassis /org/service-profile* # commit-buffer
  Firepower-chassis /org/service-profile #
  ```

  Pour mettre sous tension :

  ```
  Firepower-chassis /org/service-profile # power up
  Firepower-chassis /org/service-profile* # commit-buffer
  Firepower-chassis /org/service-profile #
  ```

- Arrêtez le châssis Au niveau de l'interface de ligne de commande de FXOS, voyez l'exemple suivant :

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

Suppression permanente

Vous pouvez supprimer définitivement un nœud de grappe en utilisant les méthodes suivantes.

- Supprimez le périphérique logique :Au niveau de l'interface de ligne de commande de FXOS, voyez l'exemple suivant :

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- Supprimez le châssis ou le module de sécurité du service : si vous mettez un périphérique hors du service, vous pouvez ajouter du matériel de remplacement en tant que nouveau nœud de la grappe.

ASA : Gérer les membres de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les membres de celle-ci.

Devenir un membre inactif

Pour devenir un membre inactif de la grappe, désactivez la mise en grappe sur le nœud tout en laissant intacte la configuration de mise en grappe.

Remarque Lorsqu'un ASA devient inactif (soit manuellement, soit à la suite d'un échec du contrôle d'intégrité), toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe; ou vous pouvez supprimer complètement le nœud de la grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), alors l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Avant de commencer

- Vous devez utiliser le port de console; vous ne pouvez pas activer ni désactiver la mise en grappe à partir d'une connexion distante d'interface de ligne de commande.
- Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 2 Désactivez la mise en grappe :

no enable

Si ce nœud était le nœud de contrôle, une nouvelle sélection de contrôle a lieu et un autre membre devient le nœud de contrôle.

La configuration de la grappe est conservée, vous pouvez donc réactiver la mise en grappe ultérieurement.

Désactiver une données

Pour désactiver un membre autre que le nœud auquel vous êtes connecté, effectuez les étapes suivantes.

Remarque Lorsqu'un ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Avant de commencer

Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.

Procédure

Supprimez le nœud de la grappe.

cluster remove unit *node_name*

La configuration de démarrage reste inchangée, ainsi que la dernière configuration synchronisée à partir du nœud de contrôle, afin que vous puissiez rajouter le nœud ultérieurement sans perdre votre configuration. Si vous saisissez cette commande sur un nœud de données pour supprimer le nœud de contrôle, un nouveau nœud de contrôle est élu.

Pour afficher les noms des membres, saisissez **cluster remove unit ?**, ou saisissez la commande **show cluster info**.

Exemple :

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement un membre, vous devez rejoindre manuellement la grappe.

Avant de commencer

- Vous devez utiliser le port de console pour réactiver la mise en grappe. Les autres interfaces sont fermées.
- Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.
- Assurez-vous que le problème est résolu avant d'essayer de rejoindre la grappe.

Procédure

Étape 1 Sur la console, passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 2 Activez la mise en grappe.

enable

Changer l'unité de contrôle

Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez spécifier le nœud exact que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez toutefois que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle à l'aide de cette procédure, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Avant de commencer

Pour le mode de contexte multiple, réalisez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, saisissez la commande **changeto system**.

Procédure

Définissez un nouveau nœud comme nœud de contrôle :

cluster control-node unit*node_name*

Exemple :

```
ciscoasa(config)# cluster control-node unit asa2
```

Vous devrez vous reconnecter à l'adresse IP de la grappe principale.

Pour afficher les noms des membres, saisissez **cluster control-node unit ?** (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exécuter une commande à l'échelle de la grappe

Pour envoyer une commande à tous les membres de la grappe ou à un membre en particulier, procédez comme suit. L'envoi d'une commande **show** à tous les membres collecte toutes les sorties et les affiche sur la console de l'unité actuelle. (Notez qu'il existe également des commandes d'affichage (show) que vous pouvez saisir sur l'unité de contrôle pour afficher les statistiques à l'échelle de la grappe.) D'autres commandes, telles que **capture** et **copy**, peuvent également profiter d'une exécution à l'échelle de la grappe.

Procédure

Envoyez une commande à tous les membres ou, si vous spécifiez le nom de l'unité, à un membre en particulier :

cluster exec [unit *unit_name*] *command*

Exemple :

```
ciscoasa# cluster exec show xlate
```

Pour afficher les noms des membres, saisissez **cluster exec unit ?** (pour afficher tous les noms à l'exception de l'unité actuelle) ou saisissez la commande **show cluster info**.

Exemples

Pour copier simultanément le même fichier de capture de toutes les unités de la grappe vers un serveur TFTP, saisissez la commande suivante sur l'unité de contrôle :

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Plusieurs fichiers PCAP, un pour chaque unité, sont copiés sur le serveur TFTP. Le nom du fichier de capture de destination est automatiquement associé au nom de l'unité, par exemple capture1_asa1.pcap, capture1_asa2.pcap, etc. Dans cet exemple, asa1 et asa2 sont des noms d'unités de grappe.

L'exemple de sortie suivant pour la commande **cluster exec show memory** affiche les renseignements sur la mémoire pour chaque membre de la grappe :

```
ciscoasa# cluster exec show memory
unit-1-1(LOCAL):*******************************************************
Free memory:      108724634538 bytes (92%)
Used memory:        9410087158 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-3:*******************************************************************
Free memory:      108749922170 bytes (92%)
Used memory:        9371097334 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-2:*******************************************************************
Free memory:      108426753537 bytes (92%)
Used memory:        9697869087 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)
```

ASA : supervision de la grappe ASA sur le Châssis Firepower 4100/9300

Vous pouvez superviser et dépanner l'état de la grappe et les connexions.

Supervision de l'état de la grappe

Consultez les commandes suivantes pour superviser l'état de la grappe :

- **show cluster info [health], show cluster chassis info**

  En l'absence de mot clé, la commande **show cluster info** affiche l'état de tous les membres de la grappe.

  La commande **show cluster info health** affiche l'intégrité actuelle des interfaces, des unités et de la grappe dans son ensemble.

  Consultez la sortie suivante pour la commande **show cluster info** :

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state SLAVE
        ID        : 1
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.1
        CCL MAC   : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
    Unit "unit-2-1" in state SLAVE
        ID        : 3
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.2.1
        CCL MAC   : 0015.c500.020f
        Last join : 20:19:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
```

- **show cluster info auto-join**

  Indique si l'unité de la grappe rejoindra automatiquement la grappe après un délai et si les conditions de défaillance (comme l'attente de la licence, l'échec de la vérification de l'intégrité du châssis, etc.) sont supprimées. Si l'unité est désactivée de façon permanente ou si l'unité est déjà dans la grappe, cette commande n'affichera aucune sortie.

  Consultez les sorties suivantes pour la commande **show cluster info auto-join** :

```
ciscoasa(cfg-cluster)# show cluster info auto-join
```

```
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport** {**asp** | **cp** [**detail**]}

  Affiche les statistiques relatives au transport pour les éléments suivants :

  - **asp** – Statistiques de transport du plan de données.
  - **cp** – Statistiques de transport du plan de commande.

    Si vous saisissez le mot clé **detail**, vous pouvez afficher l'utilisation du protocole de transport fiable de la grappe afin de cerner les problèmes d'abandon de paquet lorsque le tampon est plein dans le plan de commande. Consultez la sortie suivante pour la commande **show cluster info transport cp detail** :

    ```
    ciscoasa# show cluster info transport cp detail
    Member ID to name mapping:
      0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

    Legend:
      U    - unreliable messages
      UE   - unreliable messages error
      SN   - sequence number
      ESN  - expecting sequence number
      R    - reliable messages
      RE   - reliable messages error
      RDC  - reliable message deliveries confirmed
      RA   - reliable ack packets received
      RFR  - reliable fast retransmits
      RTR  - reliable timer-based retransmits
      RDP  - reliable message dropped
      RDPR - reliable message drops reported
      RI   - reliable message with old sequence number
      RO   - reliable message with out of order sequence number
      ROW  - reliable message with out of window sequence number
      ROB  - out of order reliable messages buffered
      RAS  - reliable ack packets sent
    ```

```
This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-----------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
```

```
  Cluster Redirect Client                          4153          73%
  Route Cluster Client                              419           7%
  RRI Cluster Client                               1105          19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                         3731         91%
  RRI Cluster Client                               328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                         3607         91%    0   0   0
  RRI Cluster Client                               317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                         578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                         572         99%
  Cluster VPN Unique ID Client                       1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

Affiche l'historique de la grappe, ainsi que les messages d'erreur indiquant pourquoi une unité de grappe n'a pas pu se joindre ou pourquoi une unité a quitté la grappe.

Capture des paquets à l'échelle de la grappe

Consultez la commande suivante pour capturer des paquets dans une grappe :

cluster exec capture

Pour prendre en charge le dépannage à l'échelle de la grappe, vous pouvez activer la capture du trafic spécifique à la grappe sur le nœud de contrôle à l'aide de la commande **cluster exec capture**, qui est ensuite automatiquement activée sur tous les nœuds de données de la grappe.

Supervision des ressources de la grappe

Consultez la commande suivante pour surveiller les ressources de la grappe :

show cluster {cpu | memory | resource} [*options*], **show cluster chassis [cpu | memory | resource usage]**

Affiche les données agrégées pour l'ensemble de la grappe. Les options disponibles dépendent du type de données.

Supervision du trafic de la grappe

Consultez la commande suivante pour superviser le trafic de la grappe :

- **show conn [detail | count], cluster exec show conn**

  La commande **show conn** indique si un flux est un flux de directeur, de sauvegarde ou de transfert. Utilisez la commande **cluster exec show conn** sur n'importe quelle unité pour afficher toutes les connexions. Cette commande peut montrer comment le trafic d'un flux unique arrive à différents ASA dans la grappe. Le débit de la grappe dépend de l'efficacité et de la configuration de l'équilibrage de charges. Cette commande offre un moyen simple d'afficher le trafic d'une connexion dans la grappe et peut vous aider à comprendre comment un équilibreur de charges peut affecter les performances d'un flux.

  Voici un exemple de sortie de la commande **show conn detail** :

```
ciscoasa/ASA2/slave# show conn detail
15 in use, 21 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
        centralized connections: 0 in use, 44 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
```

```
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
  ID 0: unit-2-1
  ID 1: unit-1-1
  ID 2: unit-1-2
  ID 3: unit-2-2
  ID 4: unit-2-3
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member
```

- **show cluster info [conn-distribution | packet-distribution | loadbalance]**

  Les commandes **show cluster info conn-distribution** et **show cluster info packet-distribution** affichent la répartition du trafic sur toutes les unités de grappe. Ces commandes peuvent vous aider à évaluer et à ajuster l'équilibreur de charges externe.

  La commande **show cluster info loadbalance** affiche les statistiques de rééquilibrage des connexions.

- **show cluster info load-monitor** [**details**]

  La commande **show cluster info load-monitor** affiche la charge de trafic pour les membres de la grappe pour le dernier intervalle ainsi que la moyenne du nombre total d'intervalles configurés (30 par défaut). Utilisez le mot clé **details** pour afficher la valeur de chaque mesure à chaque intervalle.

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 30 interval:
   0           0            0            12             28
   1           0            0            13             27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval



Connection count captured over 30 intervals:
```

```
Unit ID  0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
Unit ID  1
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0

Buffer drops captured over 30 intervals:
Unit ID  0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
Unit ID  1
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
        25         25         30         30         30         35
        25         25         35         30         30         30
        25         25         30         25         25         35
```

```
        30          30          30          25          25          25
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35


CPU usage(%) captured over 30 intervals:
Unit ID  0
        25          25          30          30          30          35
        25          25          35          30          30          30
        25          25          30          25          25          35
        30          30          30          25          25          25
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35
```

- **show cluster {access-list | conn [count] | traffic | user-identity | xlate}** [*options*], **show cluster chassis {access-list | conn | traffic | user-identity | xlate count}**

  Affiche les données agrégées pour l'ensemble de la grappe. Les options disponibles dépendent du type de données.

  Consultez la sortie suivante pour la commande **show cluster access-list** :

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
```

```
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

Pour afficher le nombre agrégé des connexions utilisées pour toutes les unités, saisissez :

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
124 in use, fwd connection 0 in use, dir connection 0 in use, centralized connection
0 in use (Cluster-wide aggregated)

unit-1-1(LOCAL):******************************************************
40 in use, 48 most used, fwd connection 0 in use, 0 most used, dir connection 0 in use,
0 most used, centralized connection 0 in use, 46 most used

unit-2-2:*************************************************************
18 in use, 40 most used, fwd connection 0 in use, 0 most used, dir connection 0 in use,
0 most used, centralized connection 0 in use, 45 most used
```

- **show asp cluster counter**

  Cette commande est utile pour le dépannage des chemins de données.

Supervision du routage de la grappe

Consultez les commandes suivantes pour le routage de la grappe :

- **show route cluster**
- **debug route cluster**

  Affiche les renseignements sur la grappe pour le routage.

- **show lisp eid**

  Affiche le tableau EID de l'ASA qui indique les EID et les ID de site.

  Consultez la sortie suivante de la commande **cluster exec show lisp eid**.

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):**************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:**************************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  Cette commande est utile pour la résolution de problèmes.

Supervision du VPN S2S distribué

Utilisez les commandes suivantes pour surveiller l'état et la répartition des sessions VPN :

- La répartition globale des sessions est fournie à l'aide de **show cluster vpn-sessiondb distribution**. Si elle est exécutée dans un environnement de contexte multiple, cette commande doit être exécutée dans l'espace d'exécution du système.

  Cette commande **show** offre un aperçu rapide des sessions, plutôt que d'avoir à exécuter **show vpn-sessiondb summary** sur chaque nœud.

- Une vue unifiée des connexions VPN sur la grappe à l'aide de la commande **show cluster vpn-sessiondb summary** est également disponible.

- La supervision des périphériques individuels à l'aide de la commande **show vpn-sessiondb** affiche le nombre de sessions actives et de sauvegarde sur un périphérique en plus des renseignements VPN habituels.

Configuration de la journalisation pour la mise en grappe

Consultez la commande suivante pour configurer la journalisation pour la mise en grappe :

logging device-id

Chaque nœud de la grappe génère des messages de journal système de manière indépendante. Vous pouvez utiliser la commande **logging device-id** pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant de nœuds identiques ou différents dans la grappe.

Débogage de la mise en grappe

Consultez les commandes suivantes pour le débogage de la mise en grappe :

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | service-module | transport]**

  Affiche les messages de débogage pour la mise en grappe.

- **debug service-module**

  Affiche les messages de débogage pour les problèmes au niveau de la lame, y compris les problèmes de vérification de l'intégrité entre le superviseur et l'application.

- **show cluster info trace**

  La commande **show cluster info trace** affiche les renseignements de débogage pour un dépannage ultérieur.

  Consultez la sortie suivante pour la commande **show cluster info trace** :

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

  Par exemple, si vous voyez les messages suivants indiquant que deux nœuds ayant le même nom **local-unit** agissent en tant que nœud de contrôle, cela peut signifier que deux nœuds ont le même nom **local-unit** (vérifiez votre configuration) ou qu'un nœud reçoit ses propres messages de diffusion (vérifiez votre réseau).

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node
 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

Dépannage du VPN S2S distribué

Notifications de VPN distribuées

Vous recevrez des messages contenant les expressions identifiées lorsque les situations d'erreur suivantes se produisent sur une grappe exécutant le VPN distribué :

Situation	Notification

Si un nœud de données de grappe existant ou en cours de connexion n'est pas en mode VPN distribué lors de la tentative de connexion à la grappe :	`Nouveau membre de la grappe (member-name) refusé en raison d'une incompatibilité de mode VPN.`
	et
	`Le nœud de contrôle (control-name) refuse la demande d'inscription de l'unité (unit-name) pour la raison suivante : les capacités du mode VPN ne sont pas compatibles avec la configuration du nœud de contrôle`

Si la licence n'est pas configurée correctement sur un membre de la grappe pour le VPN distribué :	`ERREUR : le nœud de contrôle a demandé le changement de mode VPN de la grappe sur distribué. Impossible de changer de mode en raison d'une licence d'opérateur manquante.`

Si l'horodatage ou l'ID de membre est non valide dans le SPI d'un paquet IKEv2 reçu :	`SPI expiré reçu`
	ou
	`SPI corrompu détecté`

Si la grappe ne peut pas créer de session de sauvegarde :	`Échec de la création de la sauvegarde pour une session IKEv2.`
Erreur de traitement du contact initial IKEv2 :	`Négociation IKEv2 abandonnée en raison d'une ERREUR : session de sauvegarde obsolète trouvée sur la sauvegarde`
Problèmes de redistribution :	`Échec de l'envoi du message de redistribution de session à member-name` `Échec de la réception de la réponse de déplacement de session de member-name (nœud de contrôle uniquement)`
Si la topologie change lors de la redistribution des sessions :	`Modification de la topologie de grappe détectée. Redistribution de la session VPN abandonnée.`

Vous pouvez rencontrer l'une des situations suivantes :

- Les sessions VPN de site à site sont distribuées à un seul des châssis d'une grappe lorsque le commutateur Nexus 7K est configuré avec un port de couche 4 comme algorithme d'équilibrage de charges à l'aide de la commande **port-channel load-balance src-dst l4port**. Voici un exemple d'allocation de session de grappe :

```
SSP-Cluster/data node(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
5(2501)
```

```
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

Étant donné que le VPN IKEv2 de site à site utilise le port 500 pour les ports source et de destination, les paquets IKE ne sont envoyés qu'à l'une des liaisons du canal de port connecté entre le Nexus 7K et le châssis.

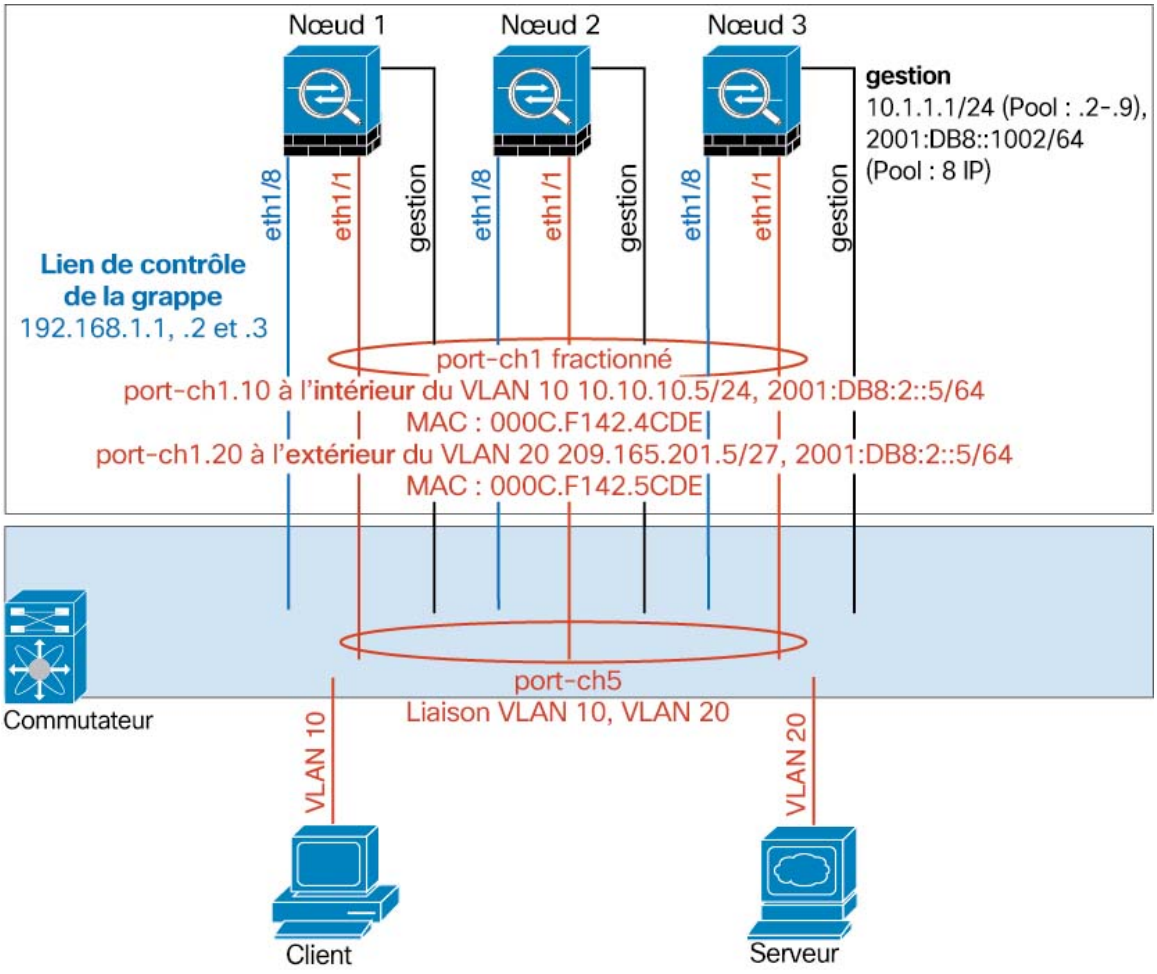
Modifiez l'algorithme d'équilibrage de charges Nexus 7K sur l'adresse IP et le port de couche 4 à l'aide de **port-channel load-balance src-dst ip-l4port**. Ensuite, les paquets IKE sont envoyés à toutes les liaisons et donc à tous les nœuds.

Pour un ajustement plus immédiat, sur le nœud de contrôle de la grappe, exécutez : **cluster redistribute vpn-sessiondb** pour redistribuer les sessions VPN actives aux nœuds de grappe des autres châssis.

Exemples de mise en grappe d'ASA

Ces exemples comprennent des déploiements typiques.

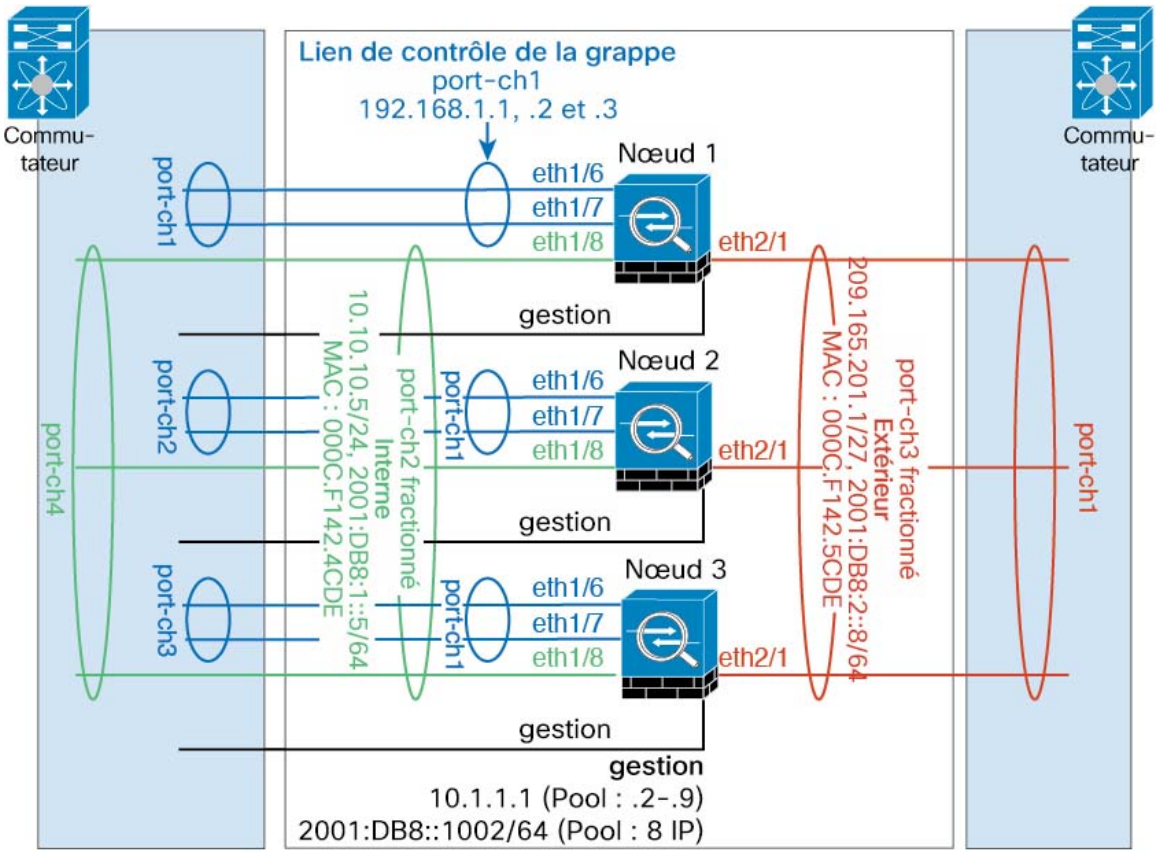
Pare-feu sur clé



Le trafic de données provenant de différents domaines de sécurité est associé à différents VLAN, par exemple, le VLAN 10 pour le réseau interne et le VLAN 20 pour le réseau externe. Chaque ASA dispose d'un seul port physique connecté au commutateur ou routeur externe. Le regroupement de liaisons est activé de sorte que tous les paquets sur la liaison physique soient encapsulés dans une norme 802.1q. L' ASA sert de pare-feu entre le VLAN 10 et le VLAN 20.

Lorsque vous utilisez des EtherChannels étendus, toutes les liaisons de données sont regroupées dans un seul EtherChannel du côté du commutateur. Si l'ASA n'est plus disponible, le commutateur rééquilibre le trafic entre les unités restantes.

Ségrégation du trafic



Vous pourriez souhaiter une séparation physique du trafic entre le réseau interne et le réseau externe.

Comme le montre le diagramme ci-dessus, il y a un EtherChannel étendu sur le côté gauche qui se connecte au commutateur interne et l'autre sur le côté droit au commutateur externe. Vous pouvez également créer des sous-interfaces VLAN sur chaque EtherChannel, au besoin.

Configuration OTV pour la mise en grappe inter-sites en mode routé

La réussite de la mise en grappe inter-sites pour le mode routé avec les EtherChannels étendus dépend de la configuration et de la supervision appropriées de l'OTV. L'OTV joue un rôle majeur en transférant les paquets sur l'interface DCI. L'OTV transfère les paquets de monodiffusion sur l'interface DCI uniquement lorsqu'il

apprend l'adresse MAC dans sa table de transfert. Si l'adresse MAC n'est pas apprise dans la table de transfert OTV, il abandonnera les paquets de monodiffusion.

Exemple de configuration OTV

```
//Sample OTV config:
//3151 - Inside VLAN, 3152 - Outside VLAN, 202 - CCL VLAN
//aaaa.1111.1234 - ASA inside interface global vMAC
//0050.56A8.3D22 - Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown
```

```
interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

Modifications du filtre OTV requises en raison d'une défaillance du site

Si un site tombe en panne, les filtres doivent être supprimés de l'OTV, car il n'est plus nécessaire de bloquer l'adresse MAC globale. Certaines configurations supplémentaires sont nécessaires.

Vous devez ajouter une entrée statique pour l'adresse MAC globale ASA sur le commutateur OTV dans le site qui est fonctionnel. Cette entrée permettra à l'OTV à l'autre extrémité d'ajouter ces entrées sur l'interface de superposition. Cette étape est nécessaire, car si le serveur et le client ont déjà l'entrée ARP pour l'ASA, ce qui est le cas pour les connexions existantes, ils n'enverront pas à nouveau l'ARP. Par conséquent, l'OTV n'aura pas la possibilité d'apprendre l'adresse MAC globale ASA dans sa table de transfert. Étant donné que l'OTV n'a pas l'adresse MAC globale dans sa table de transfert et que, conformément à sa conception, il ne diffusera pas de paquets de monodiffusion sur l'interface de superposition, il abandonnera les paquets de monodiffusion à l'adresse MAC globale du serveur, et les connexions existantes seront interrompues.

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

Lorsque l'autre site est restauré, vous devez ajouter de nouveau les filtres et supprimer cette entrée statique sur l'OTV. Il est très important d'effacer le tableau des adresses MAC dynamiques sur les deux OTV pour effacer l'entrée de superposition pour l'adresse MAC globale.

Effacement du tableau d'adresses MAC

Lorsqu'un site tombe en panne et qu'une entrée statique pour l'adresse MAC globale est ajoutée à l'OTV, vous devez laisser l'autre OTV apprendre l'adresse MAC globale sur l'interface de superposition. Une fois l'autre site rétabli, ces entrées doivent être effacées. Assurez-vous d'effacer la table d'adresses MAC pour vous assurer que l'OTV ne conserve aucune de ces entrées dans sa table de transfert.

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

Supervision du cache OTV ARP

Le service OTV gère un cache ARP pour mandataire ARP pour les adresses IP qu'il a apprises sur l'interface OTV.

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

Exemples de mise en grappe inter-sites

Les exemples suivants montrent les déploiements de grappe pris en charge.

Exemple de mode de routage EtherChannel étendu avec des adresses MAC et IP propres au site

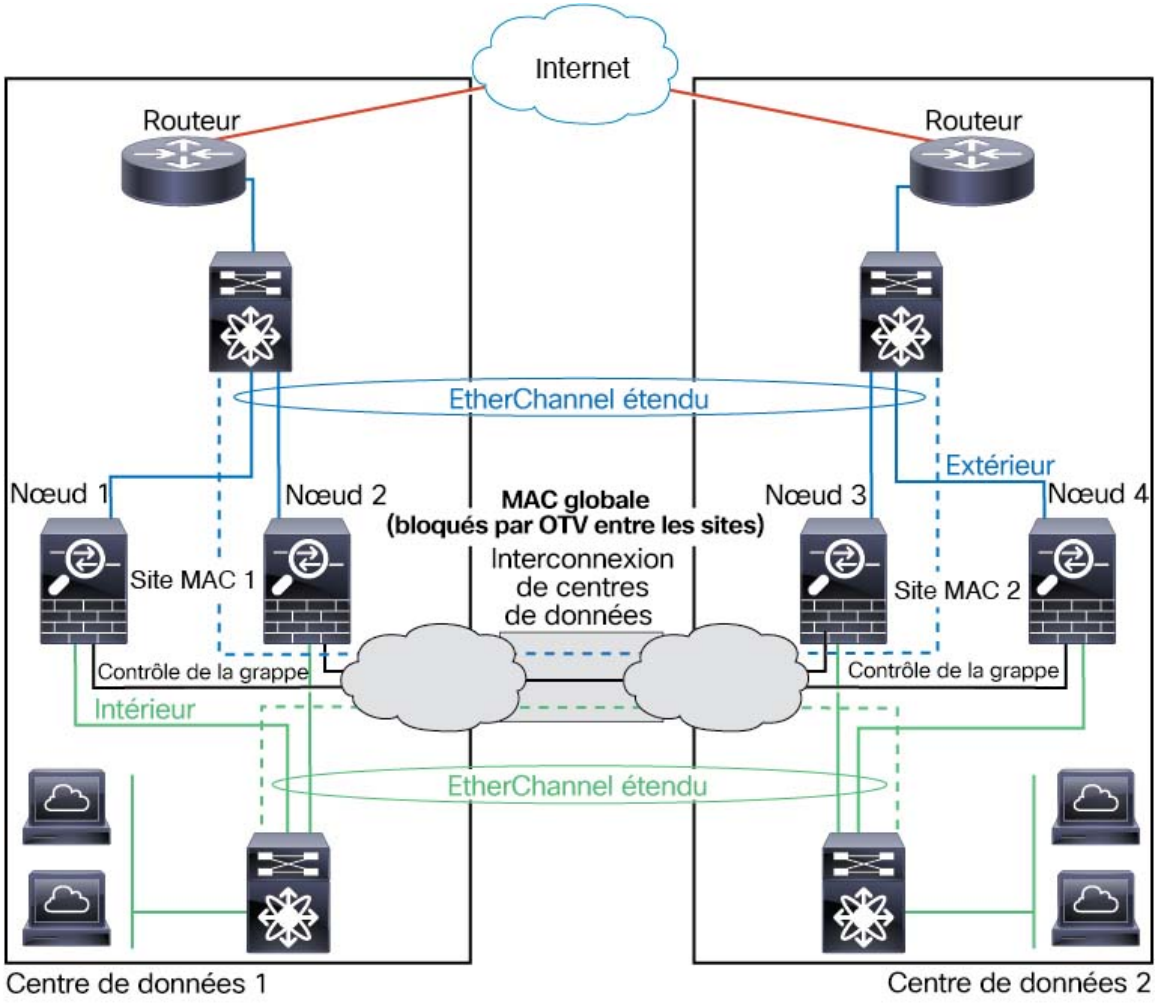
L'exemple suivant montre deux membres de la grappe dans chacun des deux centres de données, placés entre le routeur de passerelle et un réseau interne sur chaque site (insertion est-ouest). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux en utilisant des EtherChannels étendus pour le réseau interne et externe. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Les VLAN de données sont étendus entre les sites à l'aide de la virtualisation du transport par superposition (OTV) (ou d'un outil similaire). Vous devez ajouter des filtres bloquant l'adresse MAC globale pour empêcher le trafic de traverser l'interface DCI vers l'autre site lorsqu'il est destiné à la grappe. Si les nœuds de la grappe d'un site deviennent inaccessibles, vous devez supprimer les filtres pour que le trafic puisse être dirigé vers les nœuds de la grappe de l'autre site. Vous devez utiliser les adresses VACL pour filtrer l'adresse MAC globale.Pour certains commutateurs, comme le Nexus avec la carte de ligne de la gamme F3, vous devez également utiliser l'inspection ARP pour bloquer les paquets ARP de l'adresse MAC globale. L'inspection ARP nécessite que vous définissiez à la fois l'adresse MAC et l'adresse IP du site sur l'ASA. Si vous configurez uniquement l'adresse MAC du site N'oubliez pas de désactiver l'inspection ARP.

La grappe sert de passerelle pour les réseaux internes. Le MAC virtuel global, qui est partagé sur tous les nœuds de la grappe, est utilisé uniquement pour recevoir des paquets. Les paquets sortants utilisent une adresse MAC spécifique au site pour chaque grappe de contrôleurs de domaine. Cette fonctionnalité empêche les commutateurs d'apprendre la même adresse MAC globale à partir des deux sites sur deux ports différents, ce qui entraîne une oscillation MAC; au lieu de cela, ils connaissent uniquement l'adresse MAC du site.

Dans ce scénario :

- Tous les paquets de sortie envoyés par la grappe utilisent l'adresse MAC du site et sont localisés dans le centre de données.
- Tous les paquets entrants vers la grappe sont envoyés à l'aide de l'adresse MAC globale, de sorte qu'ils peuvent être reçus par n'importe quel nœud des deux sites; les filtres de l'OTV localisent le trafic dans le centre de données.



Exemple intersites nord-sud de mode transparent de l'EtherChannel étendu

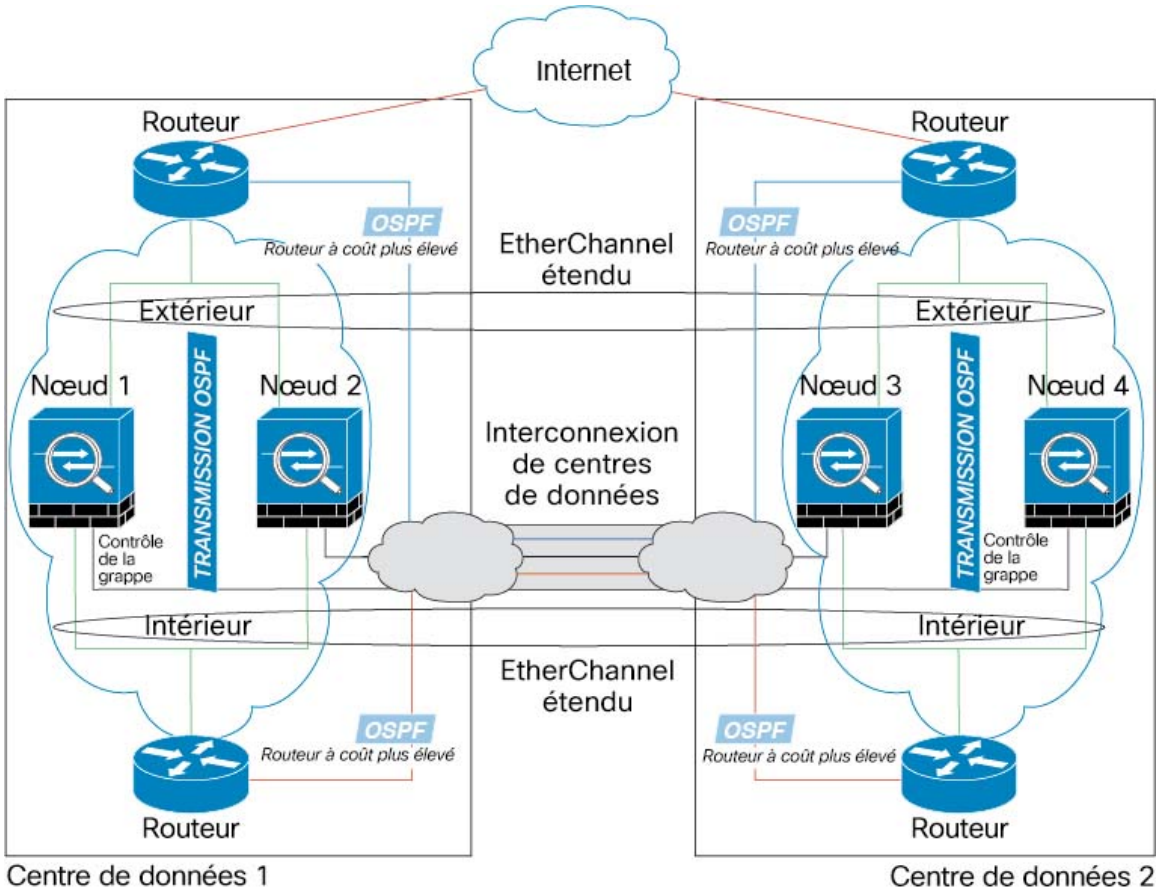
L'exemple suivant montre 2 membres de la grappe dans chacun des 2 centres de données placés entre les routeurs internes et externes (insertion nord-sud). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs

locaux en utilisant des EtherChannels étendus pour l'intérieur et l'extérieur. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Les routeurs internes et externes de chaque centre de données utilisent le protocole OSPF, qui est transmis par les périphériques ASA transparents. Contrairement aux MAC, les adresses IP des routeurs sont uniques sur tous les routeurs. En attribuant un routage à coût plus élevé sur l'interface DCI, le trafic reste dans chaque centre de données, sauf si tous les membres de la grappe d'un site donné tombent en panne. La voie de routage la moins dispendieuse qui traverse les ASA doit traverser le même groupe de ponts sur chaque site pour que la grappe puisse maintenir des connexions dissymétriques. En cas de défaillance de tous les membres de la grappe sur un site, le trafic passe de chaque routeur sur l'interface DCI aux membres de la grappe sur l'autre site.

La mise en œuvre des commutateurs sur chaque site peut inclure :

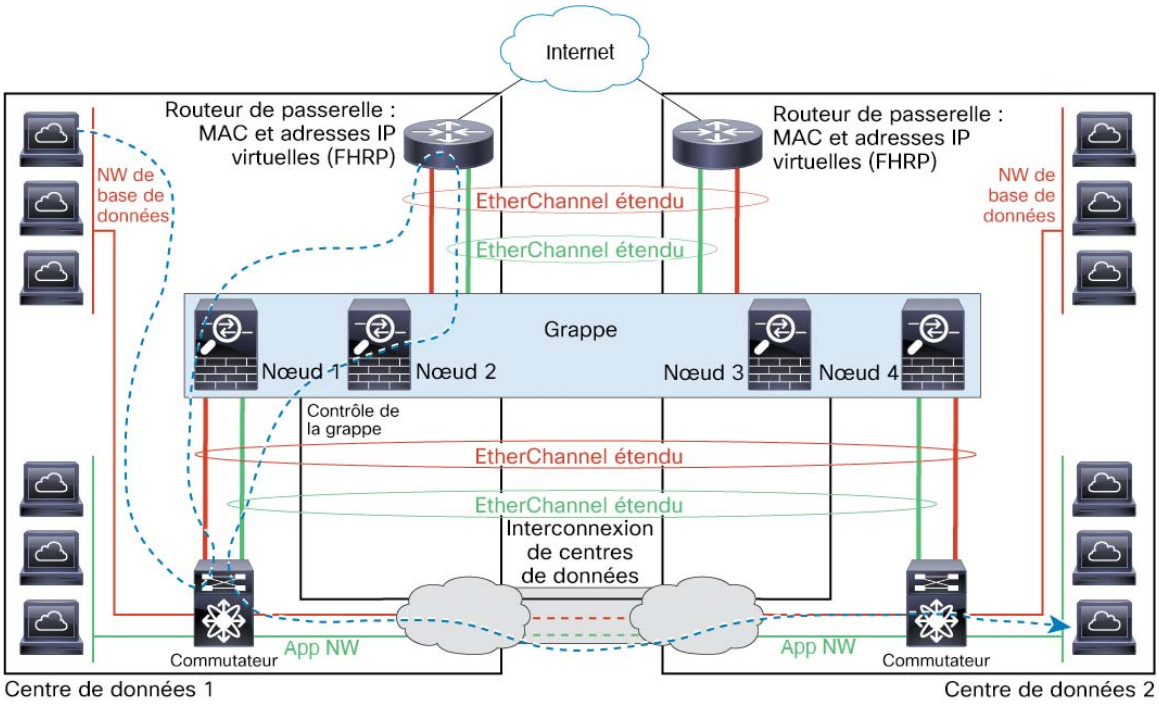
- VSS inter-sites, vPC, StackWise ou StackWise Virtual : dans ce scénario, vous installez un commutateur au centre de données 1, et l'autre au centre de données 2. Une option consiste à ce que les nœuds de la grappe de chaque centre de données se connectent uniquement au commutateur local, tandis que le trafic du commutateur redondant traverse le DCI. Dans ce cas, les connexions sont pour la plupart conservées localement à chaque centre de données. Vous pouvez éventuellement connecter chaque nœud aux deux commutateurs de la DCI si la DCI peut gérer le trafic supplémentaire. Dans ce cas, le trafic est réparti entre les centres de données, il est donc essentiel que l'interface DCI soit très robuste.
- Local VSS, vPC, StackWise ou StackWise Virtual sur chaque site : Pour une meilleure redondance des commutateurs, vous pouvez installer 2 paires de commutateurs redondants distincts sur chaque site. Dans ce cas, bien que les nœuds de la grappe aient toujours un EtherChannel étendu avec le châssis du centre de données 1 connecté uniquement aux deux commutateurs locaux et le châssis du centre de données 2 connecté à ces commutateurs locaux, l'EtherChannel étendu est essentiellement « divisé ». Chaque système de commutation local redondant voit l'EtherChannel étendu comme un EtherChannel local au site.



Exemple inter-sites est-ouest en mode transparent de l'EtherChannel étendu

L'exemple suivant montre deux membres de la grappe dans chacun des deux centres de données, placés entre le routeur de la passerelle et deux réseaux internes sur chaque site, le réseau d'applications et le réseau de base de données (insertion est-ouest). Les membres de la grappe sont connectés par la liaison de commande de grappe sur DCI. Les membres de la grappe de chaque site se connectent aux commutateurs locaux au moyen d'EtherChannels étendus pour les réseaux App et DB à l'intérieur et à l'extérieur. Chaque EtherChannel est réparti sur tous les châssis de la grappe.

Le routeur de la passerelle de chaque site utilise un FHRP comme le HSRP pour fournir les mêmes adresses MAC virtuelles et IP de destination sur chaque site. Une bonne pratique pour éviter le basculement involontaire des adresses MAC consiste à ajouter de manière statique les adresses MAC réelles des routeurs de passerelle au tableau d'adresses MAC de l'ASA à l'aide de la commande **mac-address-table static** *outside_interface mac_address*. Sans ces entrées, si la passerelle du site 1 communique avec la passerelle du site 2, ce trafic pourrait passer par l'ASA et tenter d'atteindre le site 2 à partir de l'interface interne, ce qui poserait des problèmes. Les VLAN de données sont étendus entre les sites à l'aide de la virtualisation du transport par superposition (OTV) (ou d'un outil similaire). Vous devez ajouter des filtres pour empêcher le trafic de traverser l'interface DCI vers l'autre site lorsqu'il est destiné au routeur de la passerelle. Si le routeur de la passerelle d'un site devient inaccessible, vous devez supprimer les filtres pour que le trafic puisse être dirigé vers le routeur de la passerelle de l'autre site.



Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe de l'ASA

Certaines fonctionnalités d'ASA ne sont pas prises en charge avec la mise en grappe d'ASA, et d'autres le sont uniquement sur le nœud de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

- Fonctionnalités de communication unifiée qui reposent sur le mandataire TLS
- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Interfaces de tunnel virtuel (VTI)
- Routage IS-IS
- Les inspections d'application suivantes :
  - CTIQBE
  - H323, H225 et RAS

- Intercommunication IPsec
- MGCP
- MMP
- RTSP
- SCCP (Skinny)
- WAAS
- WCCP

- Filtre de trafic de réseau de zombies
- Auto Update Server
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Équilibrage de la charge VPN
- Basculement
- Routage et pont intégrés
- Détection de connexion inactive (DCD)
- Mode FIPS

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.



Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS
  - PPTP

- RADIUS
- RSH
- SNMP
- SQLNET
- SunRPC
- TFTP
- XDMCP

- Surveillance du routage statique
- Autorisation et authentification pour l'accès réseau La comptabilité est décentralisée.
- Services de filtrage
- VPN de site à site

  En mode centralisé, les connexions VPN sont établies avec le nœud de commande de grappe uniquement. Il s'agit du mode par défaut pour la mise en grappe VPN. Le VPN de site à site peut également être déployé en mode VPN distribué, dans lequel les connexions VPN S2S IKEv2 sont réparties sur plusieurs nœuds.
- Traitement du protocole du plan de contrôle de multidiffusion IGMP (le transfert du plan de données est distribué dans la grappe)
- Traitement du protocole du plan de contrôle de multidiffusion PIM (le transfert du plan de données est distribué dans la grappe)
- Routage dynamique

Fonctionnalités appliquées aux unités individuelles

Ces fonctionnalités sont appliquées à chaque nœud ASA, plutôt qu'à la grappe dans son ensemble ou au nœud de contrôle.

- QoS : la politique QoS est synchronisée dans la grappe dans le cadre de la duplication de la configuration. Cependant, la politique est appliquée sur chaque nœud indépendamment. Par exemple, si vous configurez le contrôle en sortie, les valeurs de débit de conformité et de rafale de conformité s'appliquent au trafic sortant d'un ASA particulier. Dans une grappe à 3 nœuds et avec le trafic réparti uniformément, le taux de conformité devient en fait trois fois supérieur au débit de la grappe.
- Détection des menaces : la détection des menaces fonctionne sur chaque nœud indépendamment; par exemple, les statistiques principales sont propres au nœud. La détection de l'analyse de port, par exemple, ne fonctionne pas, car l'analyse du trafic sera équilibrée entre tous les nœuds et un nœud ne verra pas tout le trafic.
- Gestion des ressources : la gestion des ressources en mode contexte multiple est appliquée séparément sur chaque nœud en fonction de l'utilisation locale.
- Trafic LISP : le trafic LISP sur le port UDP 4342 est inspecté par chaque nœud de réception, mais aucun directeur n'est affecté. Chaque nœud ajoute au tableau EID qui est partagé dans la grappe, mais le trafic LISP lui-même ne participe pas au partage de l'état de la grappe.

AAA pour l'accès réseau et la mise en grappe

L'AAA pour l'accès réseau comprend trois composants : l'authentification, l'autorisation et la gestion de comptes. L'authentification et l'autorisation sont mises en œuvre en tant que fonctionnalités centralisées sur le nœud de contrôle de mise en grappe avec la duplication des structures de données sur les nœuds de données de grappe. Si un nœud de contrôle est choisi, le nouveau nœud de contrôle disposera de toute l'information nécessaire pour continuer le fonctionnement ininterrompu des utilisateurs authentifiés établis et de leurs autorisations associées. Les délais d'inactivité et absolue pour l'authentification des utilisateurs sont conservés lors d'un changement de nœud de contrôle se produit.

La comptabilité est mise en œuvre en tant que fonctionnalité distribuée dans une grappe. La comptabilité est effectuée flux par flux, de sorte que le nœud de la grappe possédant un flux enverra les messages de démarrage et d'arrêt de comptabilité au serveur AAA lorsque la comptabilité est configurée pour un flux.

Paramètres de connexion

Les limites de connexion s'appliquent à l'ensemble de la grappe (voir les commandes **set connection conn-max**, **set connection embryonic-conn-max**, **set connection per-client-embryonic-max**, et **set connection per-client-max**). Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.
- Si vous utilisez l'AAA pour l'accès FTP, le flux du canal de contrôle est centralisé sur le nœud de contrôle.

Inspection ICMP

Le flux des paquets d'erreurs ICMP et ICMP dans la grappe varie selon que l'inspection d'erreurs ICMP ou ICMP est activée ou non. Sans inspection ICMP, ICMP est un flux unidirectionnel et il n'y a pas de prise en charge de flux directeur. Avec l'inspection ICMP, le flux ICMP devient bidirectionnel et est soutenu par un flux directeur/de sauvegarde. L'une des différences avec un flux ICMP inspecté réside dans le traitement par le directeur du paquet transféré : le directeur transmettra le paquet de réponse d'écho ICMP au propriétaire du flux au lieu de retourner le paquet au transitaire.

Routage multidiffusion et mise en grappe

L'unité de contrôle gère tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi. Une fois la connexion établie, chaque unité de données peut transférer des paquets de données en multidiffusion.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents ASAdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les

ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à ASA qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.
- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, la grappe divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.
- Réutiliser un pool PAT dans plusieurs règles : pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion

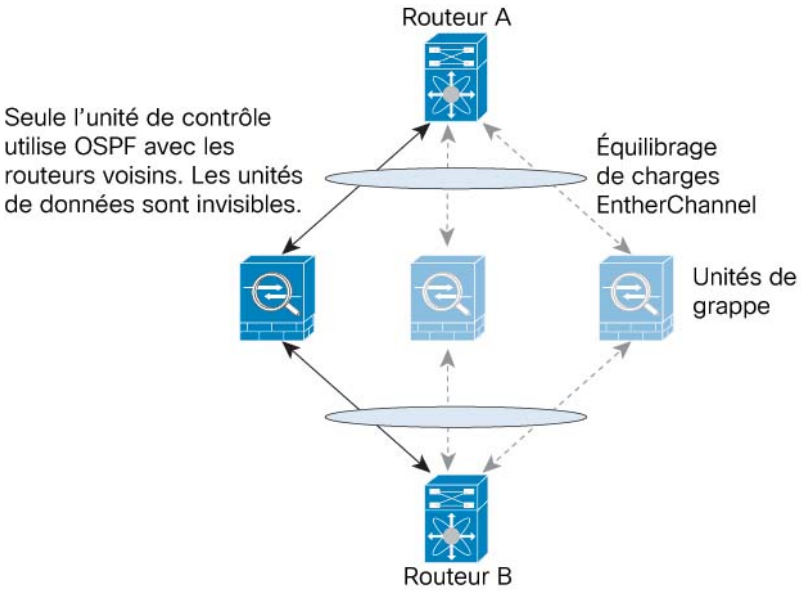
qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.

- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.
- Fonctionnalité PAT par session : bien qu'elle ne soit pas exclusive à la mise en grappe, la fonctionnalité PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque nœud de données de posséder des connexions PAT; en revanche, les connexions PAT multisessions doivent être transférées au nœud de contrôle et détenues par celui-ci. Par défaut, tout le trafic TCP et le trafic DNS UDP utilisent un xlate PAT par session, tandis que ICMP et tout le reste du trafic UDP utilise la multisession. Vous pouvez configurer des règles NAT par session pour modifier ces valeurs par défaut pour TCP et UDP, mais vous ne pouvez pas configurer la PAT par session pour ICMP. Par exemple, en raison de l'utilisation croissante du protocole Quic sur le port UDP/443 comme alternative de performance à HTTPS TLS sur TCP/443, vous devriez activer la traduction d'adresses par session (PAT) pour UDP/443. Pour le trafic qui bénéficie de la PAT multisession, comme le H.323, le SIP ou l'interface simplifiée, vous pouvez désactiver la PAT par session pour les ports TCP associés (les ports UDP de ces ports H.323 et SIP sont déjà multisession en par défaut). Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.
- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

Routage et mise en grappe dynamiques

Le processus de routage ne s'exécute que sur l'unité de contrôle, et les routages sont appris par l'unité de contrôle et répliqués sur les serveurs secondaires. Si un paquet de routage arrive à une unité de données, il est redirigé vers l'unité de contrôle.

Illustration 52 : Routage dynamique



Une fois que les unités de données ont appris les routages de l'unité de contrôle, chaque unité prend les décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée entre l'unité de contrôle et les unités de données. S'il y a un basculement de l'unité de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

SCTP et mise en grappe

Une association SCTP peut être créée sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses connexions multi-hébergement doivent résider sur le même nœud.

Inspection SIP et mise en grappe

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

La configuration du mandataire TLS n'est pas prise en charge.

SNMP et mise en grappe

Un agent SNMP interroge chaque ASA en fonction de l'adresse IP locale de son . Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud.Vous

devez les rajouter sur le nœud de contrôle pour forcer les utilisateurs à se reproduire vers le nouveau nœud, ou directement sur le nœud de données.

STUN et mise en grappe

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Syslog, NetFlow et la mise en grappe

- Syslog : chaque nœud de la grappe génère ses propres messages de journal système. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.
- NetFlow : chaque nœud de la grappe génère son propre flux NetFlow. Le collecteur NetFlow peut traiter chaque appareil ASA uniquement comme un exportateur NetFlow distinct.

Cisco TrustSec et la mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe sur le châssis Cisco Secure Firewall eXtensible Operating System (FXOS)

Une grappe ASA FXOS prend en charge l'un des deux modes mutuellement exclusifs pour le VPN de S2S, centralisé ou distribué :

- Mode VPN centralisé. Le mode par défaut. En mode centralisé, les connexions VPN sont établies avec l'unité de commande de grappe uniquement.

  La fonctionnalité VPN est limitée à l'unité de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si l'unité de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues et les utilisateurs connectés au VPN subissent une interruption de service. Lorsqu'une nouvelle unité de contrôle est choisie, vous devez rétablir les connexions VPN.

  Lorsque vous connectez un tunnel VPN à une adresse d'interface étendue, les connexions sont automatiquement transférées à l'unité de contrôle. Les clés et les certificats VPN sont répliqués sur toutes les unités.

- Mode de VPN distribué. Dans ce mode, les connexions VPN S2S IPsec IKEv2 sont réparties sur les membres d'une grappe ASA, ce qui offre une grande évolutivité. La distribution des connexions VPN entre les membres d'une grappe permet d'utiliser pleinement la capacité et le débit de la grappe, ce qui augmente considérablement la prise en charge des VPN au-delà des capacités VPN centralisées.

Remarque Le mode de mise en grappe VPN centralisée prend en charge S2S IKEv1 et S2S IKEv2.

Le mode de mise en grappe du VPN distribué prend uniquement en charge S2S, IKEv2.

Le mode de mise en grappe du VPN distribué est pris en charge sur le Firepower 9300 uniquement.

Le VPN d'accès à distance n'est pas pris en charge en mode de mise en grappe de VPN centralisé ou distribué.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, pour le débit TCP, le périphérique Firepower 9300 avec ses 3 modules SM-40 peut gérer environ 135 Gbit/s du trafic de pare-feu du monde réel lorsqu'il fonctionne seul. Pour le double châssis, le débit maximal combiné sera d'environ 80 % des 270 Gbit/s (2 châssis x 135 Gbit/s) : 216 Gbit/s.

Choix d'unité de contrôle

Les membres de la grappe communiquent sur le lien de commande de grappe pour élire une unité de contrôle comme suit :

1. Lorsque vous déployez la grappe, chaque unité diffuse une demande de sélection toutes les 3 secondes.
2. toute autre unité ayant un niveau de priorité plus élevée répondra à la demande de sélection; la priorité est définie lorsque vous déployez la grappe et n'est pas configurable.
3. Si, après 45 secondes, une unité ne reçoit pas de réponse d'une autre unité de priorité plus élevée, elle devient l'unité de contrôle.

Remarque Si plusieurs unités sont à égalité pour la priorité la plus élevée, le nom de l'unité de la grappe suivi du numéro de série est utilisé pour déterminer l'unité de contrôle.

4. Si une unité se joint ultérieurement à la grappe avec une priorité plus élevée, elle ne devient pas automatiquement l'unité de contrôle; l'unité de contrôle existante conserve toujours ses fonctions d'unité de contrôle, sauf si elle arrête de répondre, auquel cas une nouvelle unité de contrôle est élue.
5. Dans un scénario de « split-brain » (processeur partagé), où il y a temporairement plusieurs unités de contrôle, l'unité ayant la priorité la plus élevée conserve le rôle tandis que les autres unités retournent aux rôles d'unité de données.

Remarque Vous pouvez forcer manuellement une unité à devenir l'unité de contrôle. Pour les fonctions centralisées, si vous forcez le changement d'unité de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur la nouvelle unité de contrôle.

Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité du châssis, des unités et de l'interface, et en reproduisant les états de connexion entre les unités.

Surveillance des applications du châssis

La surveillance de l'intégrité de l'application du châssis est toujours activée. Le superviseur Châssis Firepower 4100/9300 vérifie l'application ASA régulièrement (à chaque seconde). Si l'ASA est opérationnel et ne peut pas communiquer avec le superviseur Châssis Firepower 4100/9300 pendant 3 secondes, l'ASA génère un message syslog et quitte la grappe.

Si le superviseur Châssis Firepower 4100/9300 ne peut pas communiquer avec l'application après 45 secondes, il recharge l'ASA. Si l'ASA ne peut pas communiquer avec le superviseur, il se supprime de la grappe.

Surveillance de l'intégrité de l'unité

Chaque unité envoie périodiquement un paquet de diffusion keepaliveheartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet keepaliveheartbeat ou autre paquet d'un nœud de données au cours de la période d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est choisi parmi le nœud restant.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle. Consultez Choix d'unité de contrôle, à la page 530 pour de plus amples renseignements.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles utilisées et signale les modifications d'état au nœud de contrôle. Pour la mise en grappe sur plusieurs châssis, les EtherChannels étendus utilisent le protocole cLACP (Link Aggregation Control Protocol). Chaque châssis surveille l'état de la liaison et les messages du protocole cLACP pour déterminer si le port est toujours actif dans l'EtherChannel et informe l'application ASA si l'interface est en panne. Lorsque vous activez la surveillance de l'intégrité, les interfaces physiques sont surveillées par défaut (y compris l'interface principale EtherChannel pour les interfaces EtherChannel). Seules les interfaces nommées qui sont dans un état activé peuvent être surveillées. Par exemple, tous les ports membres d'un EtherChannel doivent tomber en panne avant qu'un EtherChannel *nommé* ne soit supprimé de la grappe (selon votre paramètre de regroupement de ports minimal). Vous pouvez éventuellement désactiver la surveillance par interface.

Si une interface surveillée tombe en panne sur un nœud particulier, mais qu'elle est active sur d'autres nœuds, ce nœud est supprimé de la grappe. Le délai avant la suppression par ASA d'un nœud de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. L'ASA ne surveille pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de ASA de la grappe. Pour un membre établi, le nœud est supprimé après 500 ms.

Pour la mise en grappe sur plusieurs châssis, si vous ajoutez ou supprimez un EtherChannel de la grappe, la surveillance de l'intégrité de l'interface est suspendue pendant 95 secondes pour que vous ayez le temps d'effectuer les modifications sur chaque châssis.

Surveillance de l'application Decorator

Lorsque vous installez une application décorateur sur une interface, comme l'application Radware DefensePro, ASA et l'application décorateur doivent être opérationnels pour rester dans la grappe. L'unité ne rejoint pas la grappe tant que les deux applications ne sont pas opérationnelles. Une fois dans la grappe, l'unité surveille l'intégrité de l'application du séparateur toutes les 3 secondes. Si l'application décorateur est en panne, l'unité est supprimée de la grappe.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

ASA tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque ASA devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Rejoindre la grappe

Après le retrait d'un membre de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe au niveau du port de console de l'ASA en saisissant la commande **cluster group** *name*, puis **enable**.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : l'ASA essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment. Ce comportement est configurable.
- Échec de l'interface de données : l'ASA tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'ASA désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe au niveau du port de console de l'ASA en saisissant la commande **cluster group** *name*, puis **enable**.Ce comportement est configurable.
- Unité en échec : si l'unité a été supprimée de la grappe en raison d'un échec de vérification de l'intégrité de l'unité, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que l'unité rejoindra la grappe au redémarrage, à condition que la liaison de commande de grappe soit active. L'unité tente de rejoindre la grappe toutes les 5 secondes.

- Échec de la communication Châssis-Application : lorsque l'ASA détecte que l'intégrité de l'application de châssis a été récupérée, l'ASA essaie de rejoindre la grappe immédiatement.
- Échec de l'application de décorateur : l'ASA rejoint la grappe lorsqu'il détecte que l'application de décorateur est sauvegardée.
- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc. Une unité tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Ce comportement est configurable.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 19 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
Tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	Comprend les règles AAA (uauth).
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—
VPN distribué (site à site) pour Firepower 4100/9300	Oui	La session de sauvegarde devient la session active, puis une nouvelle session de sauvegarde est créée.

Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- Propriétaire du sauvegarde : nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis.

  Si vous activez la localisation du directeur pour la mise en grappe inter-sites, il existe deux rôles de propriétaire de la sauvegarde : le rôle de sauvegarde locale et de sauvegarde globale. Le propriétaire choisit toujours une sauvegarde locale sur le même site que lui (en fonction de l'ID du site). La sauvegarde globale peut se trouver sur n'importe quel site et peut même se trouver sur le même nœud que la sauvegarde locale. Le propriétaire envoie des informations sur l'état de la connexion aux deux sauvegardes.

  Si vous activez la redondance de sites et que le propriétaire de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La sauvegarde de châssis et la sauvegarde de site sont indépendantes. Par conséquent, dans certains cas, un flux comportera à la fois une sauvegarde de châssis et une sauvegarde de site.
- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Si vous activez la localisation de directeur pour la mise en grappe inter-sites, il y a deux rôles de directeur : le directeur local et le directeur global. Le propriétaire choisit toujours un directeur local sur le même site que lui (en fonction de l'ID du site). Le directeur global peut être sur n'importe quel site et peut même être le même nœud que le directeur local. En cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site.

  Détails du hachage ICMP/ICMPv6 :

  - Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.

- Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
- Pour les autres paquets, les ports source et de destination sont à 0.

- Transitaire : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Si vous activez la localisation de directeur, le redirecteur interroge toujours le directeur local. Le transitaire n'interroge le directeur global que si le directeur local ne connaît pas le propriétaire, par exemple, si un membre de la grappe reçoit des paquets pour une connexion qui appartient à un autre site. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.



Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- Propriétaire de fragment : pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Connexions par traduction d'adresse de port

Lorsqu'une connexion utilise la traduction d'adresses de port (PAT), le type de PAT (par session ou multisession) influence quel membre de la grappe devient propriétaire de la nouvelle connexion :

- PAT par session : le propriétaire est le nœud qui reçoit le paquet initial dans la connexion.

  Par défaut, le trafic TCP et DNS UDP utilise une PAT par session.

- PAT multisession : le propriétaire est toujours le nœud de contrôle. Si une connexion PAT multisession est initialement reçue par un nœud de données, le nœud de données transfère la connexion au nœud de contrôle.

  Par défaut, le trafic UDP (à l'exception du trafic UDP DNS) et ICMP utilise la PAT multisession. Ces connexions appartiennent donc toujours au nœud de contrôle.

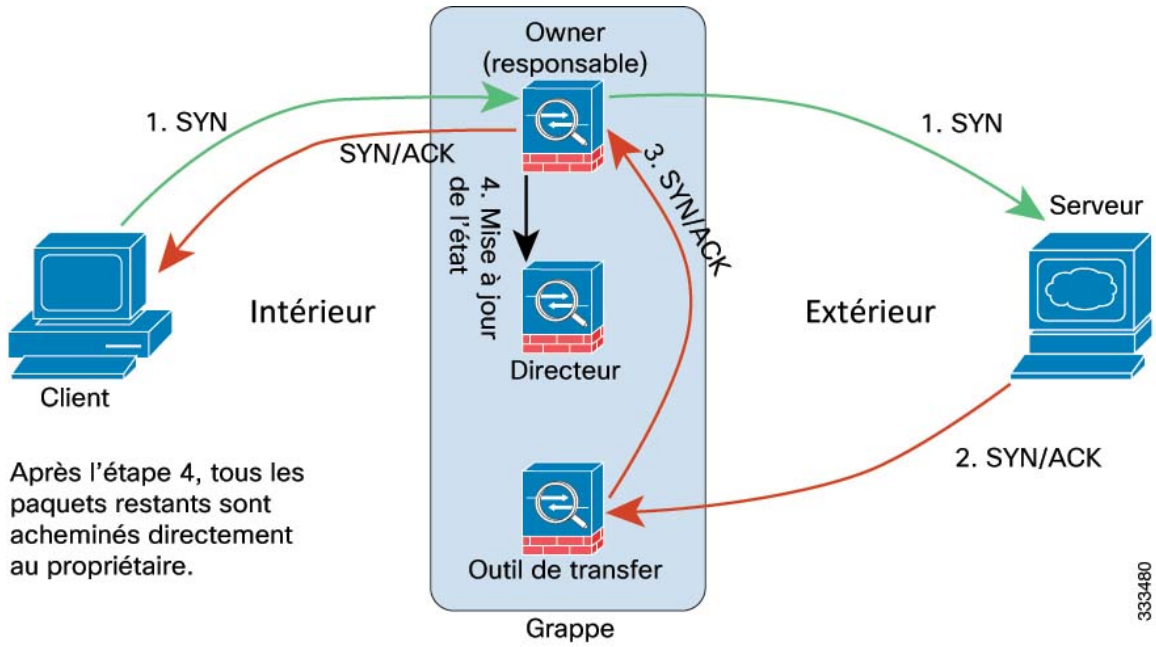
Vous pouvez modifier les valeurs par défaut de PAT par session pour les protocoles TCP et UDP afin que les connexions à ces protocoles soient gérées par session ou multisession selon la configuration. Pour ICMP, vous ne pouvez pas modifier la PAT multisession par défaut. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.



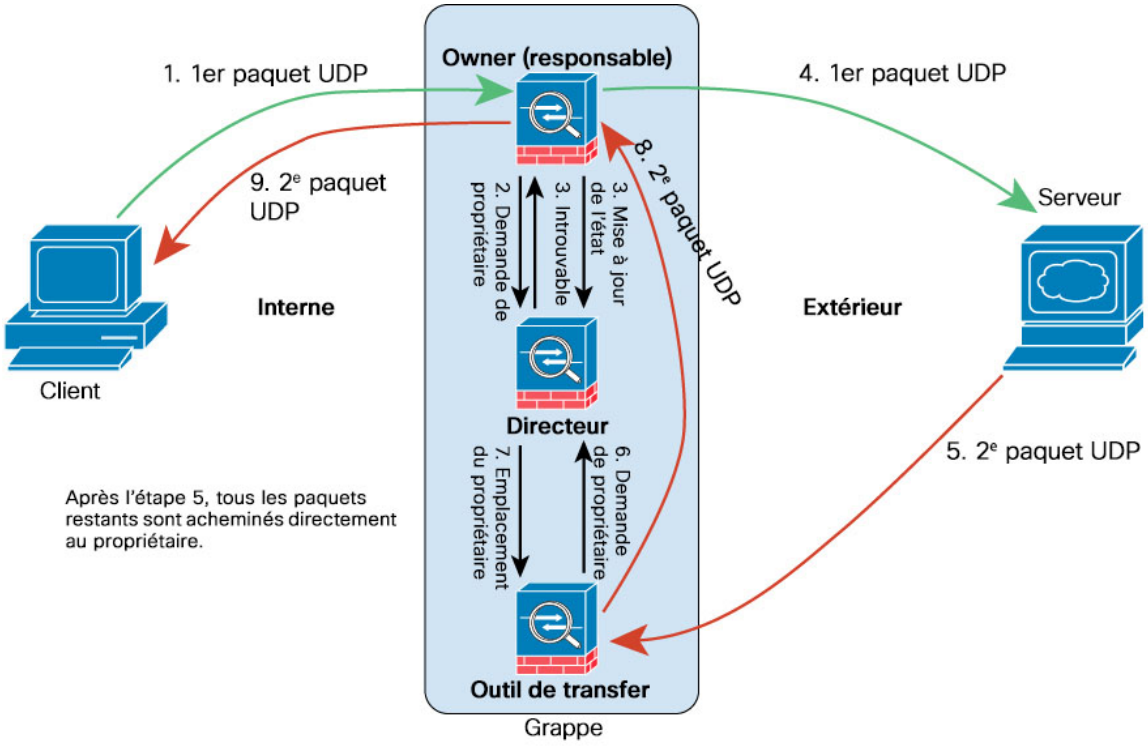
1. Le paquet SYN provient du client et est livré à un ASA (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un ASA différent (selon la méthode d'équilibrage de la charge). Cet ASA est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.
5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.

6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. ***Illustration 53 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un ASA (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.
6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.

8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Rééquilibrage des nouvelles connexions TCP dans la grappe

Si les capacités d'équilibrage de charges des routeurs en amont ou en aval entraînent une répartition non équilibrée des flux, vous pouvez configurer un rééquilibrage des nouvelles connexions afin que les nœuds ayant le plus de nouvelles connexions par seconde redirigent les nouveaux flux TCP vers d'autres nœuds. Aucun flux existant ne sera déplacé vers d'autres nœuds.

Comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Historique de la mise en grappe d'ASA sur le Firepower 4100/9300

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Suppression des propos tendancieux	9.19(1)	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
Amélioration de l'attribution des blocs de ports PAT pour la mise en grappe sur le Firepower 4100/9300	9.16(1)	L'allocation améliorée des blocs de ports PAT garantit que l'unité de contrôle conserve des ports en réserve pour les nœuds en cours de jonction et récupère de manière proactive les ports inutilisés. Pour optimiser au mieux l'allocation, vous pouvez définir le nombre maximum de nœuds que vous prévoyez d'avoir dans la grappe à l'aide de la commande **cluster-member-limit**. L'unité de contrôle peut ensuite allouer des blocs de ports au nombre de nœuds planifié sans avoir à réserver des ports pour des nœuds supplémentaires que vous ne comptez pas utiliser. La valeur par défaut est de 16 nœuds. Vous pouvez également surveiller le journal système 747046 pour vous assurer qu'il y a suffisamment de ports disponibles pour un nouveau nœud. Commandes nouvelles ou modifiées : **cluster-member-limit**, **show nat pool cluster** [**summary**], **show nat pool ip detail**
Améliorations de la commande **show cluster history**	9.16(1)	Nous avons ajouté des sorties supplémentaires pour la commande **show cluster history**. Commandes nouvelles ou modifiées : **show cluster history brief**, **show cluster history latest**, **show cluster history reverse**, **show cluster history time**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Synchronisation de la configuration avec les unités de données en parallèle	9.14(1)	L'unité de contrôle synchronise maintenant les changements de configuration avec les unités de données en parallèle par défaut. Auparavant, la synchronisation se produisait de manière séquence. Commandes nouvelles ou modifiées : **config-replicate-parallel**
Messages pour un échec de jonction de grappe ou une éviction ajoutés à **show cluster history**	9.14(1)	De nouveaux messages ont été ajoutés à la commande **show cluster history** lorsqu'une unité de grappe ne parvient pas à rejoindre la grappe ou la quitter. Commandes nouvelles ou modifiées : **show cluster history**
Informations sur l'initiateur et le répondeur pour la détection des connexions inactives (DCD) et prise en charge du DCD dans une grappe.	9.13(1)	Si vous activez la détection des connexions inactives (DCD), vous pouvez utiliser la commande **show conn detail** pour obtenir des informations sur l'initiateur et le répondeur. La détection des connexions inactives vous permet de maintenir une connexion inactive, et la sortie **show conn** vous indique la fréquence à laquelle les points terminaux ont été sondés. En outre, DCD est désormais pris en charge dans une grappe. Commandes nouvelles ou modifiées : **show conn** (sortie uniquement).
Superviser la charge de trafic pour une grappe	9.13(1)	Vous pouvez désormais superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur l'unité si les unités restantes peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Commandes nouvelles/modifiées : **debug cluster load-monitor**, **load-monitor**, **show cluster info load-monitor**
Jonction de grappe accélérée	9.13(1)	Lorsqu'une unité de données a la même configuration que l'unité de contrôle, elle ignorera la synchronisation de la configuration et se joindra plus rapidement. Cette fonction est activée par défaut. Cette fonctionnalité est configurée sur chaque unité et n'est pas répliquée de l'unité de contrôle à l'unité de données. **Remarque** Certaines commandes de configuration ne sont pas compatibles avec la jonction accélérée de grappes; si ces commandes sont présentes sur l'unité, même si la jonction accélérée de grappes est activée, la synchronisation de la configuration se produira toujours. Vous devez supprimer la configuration incompatible pour que la jonction accélérée de grappes fonctionne. Utilisez la commande **show cluster info unit-join-acceleration incompatible-config** pour afficher la configuration incompatible. Commandes nouvelles/modifiées : **unit join-acceleration**, **show cluster info unit-join-acceleration incompatible-config**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Protocole ARP gratuit par site pour la mise en grappe	9.12(1)	L'ASA génère maintenant des paquets ARP gratuits (GARP) pour maintenir l'infrastructure de commutation à jour : le membre ayant la priorité la plus élevée sur chaque site génère périodiquement du trafic GARP pour les adresses MAC et IP globales. Lorsque vous utilisez des adresses MAC et IP par site, les paquets provant de la grappe utilisent une adresse MAC et une adresse IP propres au site, tandis que les paquets reçus par la grappe utilisent une adresse MAC et une adresse IP globales. Si le trafic n'est pas généré périodiquement à partir de l'adresse MAC globale, vous pourriez rencontrer un délai d'expiration de l'adresse MAC sur vos commutateurs pour l'adresse MAC globale. Après un délai d'expiration, le trafic destiné à l'adresse MAC globale sera inondé dans l'ensemble de l'infrastructure de commutation, ce qui peut entraîner des problèmes de performance et de sécurité. Le GARP est activé par défaut lorsque vous définissez l'ID de site pour chaque unité et l'adresse MAC du site pour chaque EtherChannel étendu. Commandes nouvelles ou modifiées : **site-periodic-garp interval**
Groupement d'unités de grappe en parallèle par châssis Firepower 9300	9.10(1)	Pour Firepower 9300, cette fonctionnalité garantit que les modules de sécurité d'un châssis rejoignent la grappe simultanément afin que le trafic soit réparti uniformément entre les modules. Si un module se joint très avant les autres modules, il peut recevoir plus de trafic que souhaité, car les autres modules ne peuvent pas encore partager la charge. Commandes nouvelles ou modifiées : **unit parallel-join**
Adresse IP personnalisable par liaison de commande de grappe pour le Firepower 4100/9300	9.10(1)	Par défaut, la liaison de commande de grappe utilise le réseau 127.2.0.0/16. Vous pouvez maintenant définir le réseau lorsque vous déployez la grappe dans FXOS. Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot_id*. Cependant, certains déploiements réseau ne permettent pas le passage du trafic 127.2.0.0/16. Par conséquent, vous pouvez maintenant définir un sous-réseau personnalisé /16 pour la liaison de commande de grappe dans FXOS, à l'exception des adresses de boucle avec retour (127.0.0.0/8) et de multidiffusion (224.0.0.0/4). Commandes FXOS nouvelles ou modifiées : **set cluster-control-link network**
Le délai de réponse de l'interface de grappe s'applique désormais aux interfaces qui passent d'un état inactif à un état opérationnel.	9.10(1)	Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié dans la commande **health-check monitor-interface debounce-time** ou dans l'écran **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** d'ASDM avant de marquer l'interface comme ayant échoué et que l'unité soit supprimée de la grappe. Cette fonctionnalité s'applique désormais aux interfaces qui passent d'un état inactif à un état opérationnel. Par exemple, dans le cas d'un EtherChannel qui passe d'un état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un délai de réponse plus long peut empêcher l'interface de sembler être défaillante sur une unité de la grappe juste parce qu'une autre unité de la grappe a été plus rapide à regrouper les ports. Nous n'avons pas modifié de commandes.

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Rejoindre automatiquement la grappe après une défaillance interne	9.9(2)	Auparavant, de nombreuses conditions d'erreur entraînaient le retrait d'une unité de la grappe et vous deviez rejoindre manuellement la grappe après avoir résolu le problème. Désormais, une unité tentera de rejoindre la grappe automatiquement aux intervalles suivants par défaut : 5 minutes, 10 minutes, puis 20 minutes. Ces valeurs sont configurables. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite. Commandes nouvelles ou modifiées : **health-check system auto-rejoin, show cluster info auto-join**
Afficher les statistiques relatives au transport pour les messages du protocole de transport fiable de la grappe	9.9(2)	Vous pouvez désormais afficher l'utilisation du tampon de transport fiable par grappe d'unités afin de cerner les problèmes d'abandon de paquet lorsque le tampon est plein dans le plan de commande. Commande nouvelle ou modifiée : **show cluster info transport cp detail**
Le comportement de la commande **cluster remove unit** correspond au comportement **no enable**	9.9(1)	La commande **cluster remove unit** supprime maintenant une unité de la grappe jusqu'à ce que vous réactiviez manuellement la mise en grappe ou la rechargiez, de manière similaire à la commande **no enable**. Auparavant, si vous redéployiez la configuration de démarrage à partir de FXOS, la mise en grappe était réactivée. Désormais, l'état désactivé persiste même dans le cas d'un redéploiement de la configuration de démarrage. Cependant, le rechargement de l'ASA réactivera la mise en grappe. Commande nouvelle ou modifiée : **cluster remove unit**
Amélioration de la détection des échecs de vérification de l'intégrité du châssis	9.9(1)	Vous pouvez désormais configurer un délai de rétention inférieur pour la vérification de l'intégrité du châssis : 100 ms. Le minimum précédent était de 300 ms. Notez que la durée minimum combinée (*intervalle* x *nombre de tentatives*) ne peut pas être inférieure à 600 ms. Commande nouvelle ou modifiée : **app-agent heartbeat interval**
Redondance inter-sites pour la mise en grappe	9.9(1)	La redondance inter-sites garantit qu'un propriétaire de secours pour un flux de trafic se trouvera toujours sur l'autre site que le propriétaire. Cette fonctionnalité offre une protection contre les défaillances du site. Commande nouvelle ou modifiée : **site-redundancy, show asp cluster counter change, show asp table cluster chash-table, show conn flag**
VPN de site à site distribué avec mise en grappe sur le Firewall 9300	9.9(1)	Une grappe ASA sur le Firewall 9300 prend en charge le VPN de site à site en mode distribué. Le mode distribué permet d'avoir de nombreuses connexions VPN IPsec IKEv2 de site à site réparties sur les membres d'une grappe ASA, pas seulement sur l'unité de contrôle (comme en mode centralisé). Cela étend considérablement la prise en charge des VPN au-delà des capacités VPN centralisées et offre une haute disponibilité. Le VPN S2S distribué s'exécute sur une grappe allant jusqu'à deux châssis, chacun contenant jusqu'à trois modules (six membres de grappe au total), chaque module prenant en charge jusqu'à 6 000 sessions actives (12 000 au total), pour un maximum d'environ 36 000 sessions actives (72 000 au total). Commandes ajoutées ou modifiées : **cluster redistribute vpn-sessiondb**, **show cluster vpn-sessiondb**, **vpn mode**, **show cluster resource usage**, **show vpn-sessiondb**, **show connection detail**, **show crypto ikev2**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Détection améliorée des échecs de vérification de l'intégrité de l'unité de grappe	9.8(1)	Vous pouvez maintenant configurer un délai de rétention inférieur pour la vérification de l'intégrité de l'unité : 0,3 seconde au minimum. La valeur minimum précédente était de 0,8 seconde. Cette fonctionnalité modifie le schéma de messagerie de vérification de l'intégrité de l'unité pour passer des *keepalives* dans le plan de commande aux *heartbeats* dans le plan de données. L'utilisation de pulsations améliore la fiabilité et la réactivité de la mise en grappe en évitant les problèmes liés à la surcharge du processeur du plan de commande et aux retards de planification. Notez que la configuration d'un délai de rétention inférieur augmente l'activité de messagerie de la liaison de commande de grappe. Nous vous suggérons d'analyser votre réseau avant de configurer un faible délai de rétention. Par exemple, assurez-vous que l'envoi d'un message Ping d'une unité à une autre via la liaison de commande de grappe retourne dans le *holdtime*/3, car il y aura trois messages de pulsation au cours d'un intervalle de délai de rétention. Si vous rétrogradez votre logiciel ASA après avoir défini le délai de rétention sur 0,3–0,7, ce paramètre reviendra à la valeur par défaut de 3 secondes, car le nouveau paramètre n'est pas pris en charge. Nous avons modifié les commandes suivantes : **health-check holdtime, show asp drop cluster counter, show cluster info health details**
Délai anti-rebond configurable pour marquer une interface comme défaillante pour l'Châssis Firepower 4100/9300	9.8(1)	Vous pouvez maintenant configurer le délai antirebond avant que l'ASA considère une interface comme défaillante et que l'unité ne soit supprimée de la grappe. Cette fonctionnalité permet une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme défaillante, et l'unité est supprimée de la grappe. Le délai antirebond par défaut est de 500 ms, avec une plage de 300 ms à 9 secondes. Commande nouvelle ou modifiée : **health-check monitor-interface debounce-time**
Amélioration de la mise en grappe inter-sites pour l'ASA sur le Châssis Firepower 4100/9300	9.7(1)	Vous pouvez maintenant configurer l'ID de site pour chaque Châssis Firepower 4100/9300 lorsque vous déployez la grappe ASA. Auparavant, vous deviez configurer l'ID de site dans l'application ASA; cette nouvelle fonctionnalité facilite le déploiement initial. Notez que vous ne pouvez plus définir l'ID de site dans la configuration ASA. En outre, pour une meilleure compatibilité avec la mise en grappe inter-sites, nous vous recommandons de mettre à niveau vers ASA 9.7(1) et FXOS 2.1.1, ce qui comprend plusieurs améliorations de la stabilité et des performances. Nous avons modifié la commande suivante : **site-id**
Localisation de directeur : amélioration de la mise en grappe inter-sites pour les centres de données	9.7(1)	Pour améliorer les performances et conserver le trafic sur un site de mise en grappe inter-sites pour les centres de données, vous pouvez activer la localisation de directeur. Les nouvelles connexions sont généralement équilibrées et appartiennent aux membres de la grappe d'un site donné. Cependant, l'ASA attribue le rôle de directeur à un membre sur *n'importe quel* site. La localisation du directeur permet des rôles de directeur supplémentaires : un directeur local sur le même site que le propriétaire et un directeur global qui peut se trouver sur n'importe quel site. Le fait de maintenir le propriétaire et le directeur sur le même site améliore les performances. En cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site. Le directeur global est utilisé si un membre d'une grappe reçoit des paquets pour une connexion appartenant à un autre site. Nous avons introduit ou modifié les commandes suivantes : **director-localization, show asp table cluster chash, show conn, show conn detail**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge de 16 châssis pour le Firepower 4100	9.6(2)	Vous pouvez maintenant ajouter jusqu'à 16 châssis à la grappe pour le Firepower 4100. Nous n'avons pas modifié de commandes.
Prise en charge de Firepower 4100	9.6(1)	Avec FXOS 1.1.4, l'ASA prend en charge la mise en grappe inter-châssis sur le Firepower 4100 pour un maximum de 6 châssis. Nous n'avons pas modifié de commandes.
Prise en charge des adresses IP spécifiques au site en mode routé avec EtherChannel étendu	9.6(1)	Pour la mise en grappe inter-sites en mode routé avec les canaux EtherChannels étendus, vous pouvez désormais configurer l'adresse IP spécifique au site en plus des adresses MAC spécifiques au site. L'ajout d'adresses IP de site vous permet d'utiliser l'inspection ARP sur les périphériques Overlay Transport Virtualization (OTV) pour empêcher les réponses ARP de l'adresse MAC globale de circuler sur l'interconnexion de centre de données (DCI), ce qui peut causer des problèmes de routage. L'inspection ARP est requise pour certains commutateurs qui ne peuvent pas utiliser de VACL pour filtrer les adresses MAC. Nous avons modifié les commandes suivantes : **mac-address, show interface**
Mise en grappe inter-châssis pour 16 modules et mise en grappe inter-sites pour l'application ASA Firepower 9300	9.5(2.1)	Grâce à FXOS 1.1.3, vous pouvez désormais activer la mise en grappe inter-châssis et par extension inter-sites. Vous pouvez inclure jusqu'à 16 modules. Par exemple, vous pouvez utiliser 1 module dans 16 châssis, ou 2 modules dans 8 châssis, ou toute combinaison qui fournit un maximum de 16 modules. Nous n'avons pas modifié de commandes.
Adresses MAC spécifiques au site pour la prise en charge de la mise en grappe inter-sites pour EtherChannel étendu en mode de pare-feu routé	9.5(2)	Vous pouvez désormais utiliser la mise en grappe inter-sites pour les EtherChannels étendus en mode routé. Pour éviter le basculement des adresses MAC, configurez un ID de site pour chaque membre d'une grappe afin qu'une adresse MAC propre au site pour chaque interface puisse être partagée entre les unités d'un site. Nous avons introduit ou modifié les commandes suivantes : **site-id, mac-address site-id, show cluster info, show interface**
Personnalisation de la grappe ASA du comportement de reconnexion automatique en cas de défaillance d'une interface ou de la liaison de commande de grappe	9.5(2)	Vous pouvez désormais personnaliser le comportement de reconnexion automatique en cas de défaillance d'une interface ou de la liaison de commande de grappe. Nous avons introduit la commande suivante : **health-check auto-rejoin**
La grappe ASA prend en charge GTPv1 et GTPv2	9.5(2)	La grappe ASA prend désormais en charge l'inspection GTPv1 et GTPv2. Nous n'avons pas modifié de commandes.
Délai de réplication de la grappe pour les connexions TCP	9.5(2)	Cette fonctionnalité aide à éliminer le « travail inutile » lié aux flux de courte durée en retardant la création du flux directeur/de sauvegarde. Nous avons introduit la commande suivante : **cluster replication delay**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Inspection LISP pour la mobilité des flux inter-sites	9.5(2)	L'architecture Cisco Locator/Protocole de séparation d'ID (LISP) sépare l'identité de l'appareil de son emplacement dans deux espaces de numérotation différents, ce qui rend la migration du serveur transparente pour les clients. L'ASA peut inspecter le trafic LISP pour détecter les changements d'emplacement, puis utiliser ces renseignements pour un fonctionnement de mise en grappe transparent; les membres de la grappe ASA inspectent le trafic LISP passant entre le routeur de premier saut et le routeur de tunnel de sortie (ETR) ou le routeur de tunnel de sortie (ITR), puis changent le propriétaire du flux pour qu'il se trouve sur le nouveau site. Nous avons introduit ou modifié les commandes suivantes : **allowed-eid, clear cluster info flow-mobility counters, clear lisp eid, cluster flow-mobility lisp, debug cluster flow-mobility, debug lisp eid-notify-intercept, flow-mobility lisp, inspect lisp, policy-map type inspect lisp, site-id, show asp table classify domain inspect-lisp, show cluster info flow-mobility counters, show conn, show lisp eid, show service-policy, validate-key**
Les améliorations de la NAT de classe opérateur sont désormais prises en charge dans le basculement et la mise en grappe d'ASA	9.5(2)	Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Cette fonctionnalité est désormais prise en charge dans les déploiements de basculement et de grappe ASA. Nous avons modifié la commande suivante : **show local-host**
Niveau configurable pour la mise en grappe des entrées de trace	9.5(2)	Par défaut, tous les niveaux d'événements de mise en grappe sont inclus dans le tampon de trace, y compris de nombreux événements de bas niveau. Pour limiter la trace aux événements de niveau supérieur, vous pouvez définir le niveau de trace minimum pour la grappe. Nous avons introduit la commande suivante : **trace-level**
Mise en grappe d'ASA intra-châssis pour le Firepower 9300	9.4(1.150)	Vous pouvez mettre en grappe jusqu'à 3 modules de sécurité dans le châssis Firepower 9300. Tous les modules dans le châssis doivent appartenir à la grappe. Nous avons introduit les commandes suivantes : **cluster replication delay, debug service-module, management-only individual, show cluster chassis**



CHAPITRE 12

Grappe ASA pour l'ASA virtuel pour le cloud privé

La mise en grappe vous permet de regrouper plusieurs ASA virtuel en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. Vous pouvez déployer les grappes ASA virtuel à l'aide de :

- KVM
- VMware

Remarque Seul le mode pare-feu routé est pris en charge.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 598.

- À propos de la mise en grappe d'ASA virtuel, à la page 546
- Licences pour la mise en grappe d'ASA virtuel, à la page 552
- Exigences et conditions préalables à la mise en grappe d'ASA virtuel, à la page 552
- Lignes directrices de la mise en grappe d'ASA virtuel, à la page 553
- Configurer la mise en grappe d'ASA virtuel à l'aide d'une configuration Day0, à la page 554
- Configurer la mise en grappe ASA virtuel après le déploiement, à la page 557
- Personnaliser l'opération de mise en grappe, à la page 570
- Gérer les nœuds de la grappe, à la page 581
- Supervision de la grappe ASA virtuel, à la page 586
- Exemples de mise en grappe d'ASA virtuel, à la page 597
- Référence pour la mise en grappe, à la page 598
- Historique de la mise en grappe d'ASA virtuel, à la page 614

À propos de la mise en grappe d'ASA virtuel

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

Intégration de la grappe dans votre réseau

La grappe se compose de plusieurs pare-feu agissant comme un seul périphérique. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau isolé pour la communication intra-grappe, appelé *liaison de commande de grappe*, qui utilise des interfaces VXLAN. Les VXLAN, qui agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3, permettent à la ASA virtuel d'envoyer des messages en diffusion ou en multidiffusion sur la liaison de commande de grappe.
- Accès de gestion à chaque pare-feu pour la configuration et la surveillance. Le déploiement ASA virtuel comprend une interface de gestion Management 0/0 que vous utiliserez pour gérer les nœuds de la grappe.

Lorsque vous placez la grappe dans votre réseau, les routeurs en amont et en aval doivent être en mesure d'équilibrer la charge des données entrant et provenant de la grappe à l'aide des interfaces individuelles de couche 3 et de l'une des méthodes suivantes :

- Routage basé sur les politiques : les routeurs en amont et en aval équilibrent la charge entre les nœuds à l'aide de cartes de routage et de listes de contrôle d'accès.
- Routage à chemins multiples à coût égal : les routeurs en amont et en aval effectuent l'équilibrage de la charge entre les nœuds à l'aide de routes statiques ou dynamiques à coût égal.

Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Nœuds de la grappe

Les membres du nœud collaborent pour partager la politique de sécurité et les flux de trafic. Cette section décrit la nature du rôle de chaque nœud.

Configuration du démarrage

Sur chaque appareil, vous configurez une configuration de démarrage minimale qui inclut le nom de la grappe, l'interface de la liaison de commande de grappe et les autres paramètres de la grappe. Le premier nœud sur lequel vous activez la mise en grappe devient généralement le nœud de *contrôle*. Lorsque vous activez la mise en grappe sur les nœuds suivants, ils rejoignent la grappe en tant que nœuds de *données*.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité dans la configuration de démarrage. la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds de données. En règle générale, lorsque vous créez une grappe pour la première fois, le premier nœud que vous ajoutez devient le nœud de contrôle simplement parce que c'est le seul nœud de la grappe à ce moment-là.

Vous devez effectuer toute la configuration (à l'exception de la configuration de démarrage) sur le nœud de contrôle uniquement; la configuration est ensuite reproduite sur les nœuds de données. Dans le cas de ressources physiques, telles que les interfaces, la configuration du nœud de contrôle est reflétée sur tous les nœuds de données. Par exemple, si vous configurez Ethernet 1/2 comme interface interne et Ethernet 1/1 comme interface externe, ces interfaces sont également utilisées sur les nœuds de données en tant qu'interfaces interne et externe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

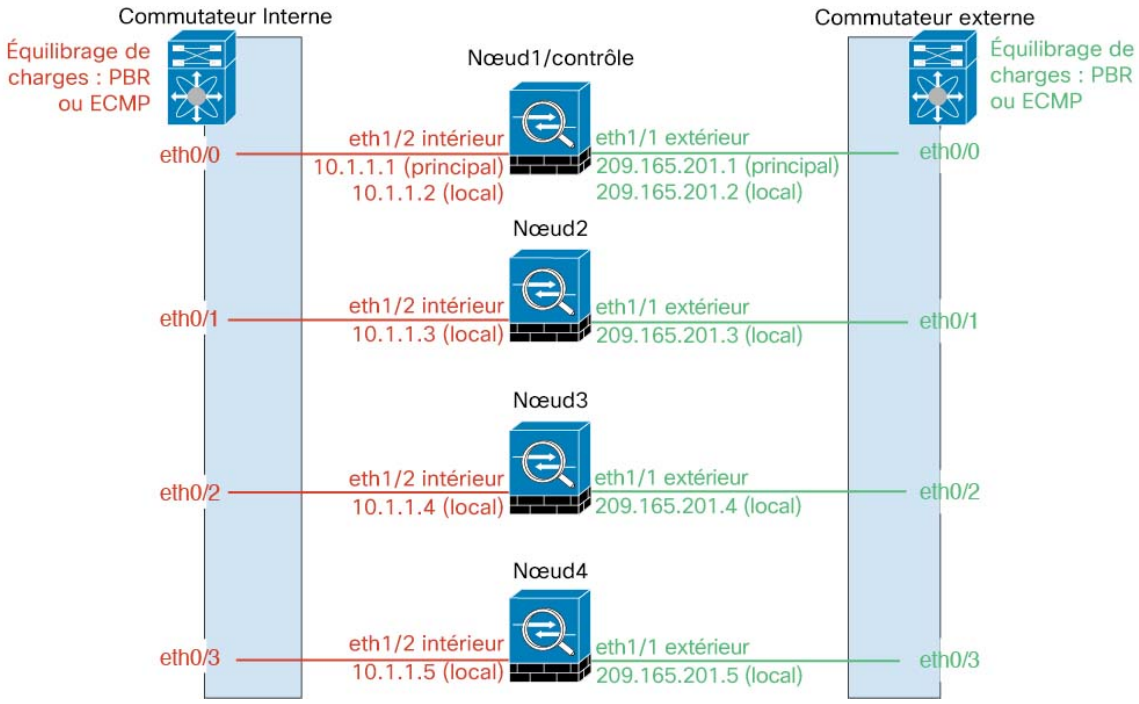
Interfaces individuelles

Vous pouvez configurer les interfaces de grappe en tant *qu'interfaces individuelles*.

Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre *adresse IP locale* utilisée pour le routage. L'*adresse IP de la grappe principale* pour chaque interface est une adresse fixe qui appartient toujours au nœud de contrôle. Lorsque le nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente.

Comme la configuration de l'interface doit être configurée uniquement sur le nœud de contrôle, vous configurez un ensemble d'adresses IP à utiliser pour une interface donnée sur les nœuds de la grappe, y compris un pour le nœud de contrôle.

L'équilibrage de charge doit être configuré séparément sur le commutateur en amont.



Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Routage à base de règles

Lorsque vous utilisez des interfaces individuelles, chaque interface ASA conserve ses propres adresses IP et MAC. Une méthode d'équilibrage de la charge est le routage basé sur les politiques (PBR).

Nous vous recommandons cette méthode si vous utilisez déjà PBR et que vous souhaitez tirer parti de votre infrastructure existante.

PBR prend des décisions de routage en fonction d'une carte de routage et d'une ACL. Vous devez répartir manuellement le trafic entre toutes les ASA d'une grappe. Comme PBR est statique, il se peut qu'il ne permette pas d'atteindre un résultat d'équilibrage de la charge optimale à tout moment. Pour obtenir les meilleures performances, nous vous recommandons de configurer la politique PBR de sorte que les paquets d'acheminement et de retour d'une connexion soient dirigés vers la même ASA. Par exemple, si vous avez un routeur Cisco, la redondance peut être obtenue en utilisant Cisco IOS PBR avec Object Tracking. Le suivi d'objets Cisco IOS surveille chaque ASA à l'aide d'un ping ICMP. PBR peut ensuite activer ou désactiver les cartes de routage en fonction de l'accessibilité d'un ASA. Consultez les URL suivantes pour en savoir plus :

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

Routage à chemins multiples à coût égal

Lorsque vous utilisez des interfaces individuelles, chaque interface ASA conserve ses propres adresses IP et MAC. Le routage à chemins multiples à coûts égaux (ECMP) est une méthode d'équilibrage de la charge.

Nous vous recommandons cette méthode si vous utilisez déjà ECMP et que vous souhaitez tirer parti de votre infrastructure existante.

Le routage ECMP peut transférer des paquets sur plusieurs « meilleurs chemins » qui se partagent la première place dans la mesure du routage. Comme pour l'EtherChannel, un hachage des adresses IP source et de destination ou des ports source et de destination peut être utilisé pour envoyer un paquet vers l'un des sauts suivants. Si vous utilisez des routes statiques pour le routage ECMP, la défaillance de ASA peut provoquer des problèmes. le routage continue d'être utilisé et le trafic vers le ASA défaillant sera perdu. Si vous utilisez des routes statiques, veillez à utiliser une fonctionnalité de surveillance de routage statique telle que le suivi d'objets. Nous recommandons d'utiliser des protocoles de routage dynamique pour ajouter et supprimer des routes, auquel cas vous devez configurer chaque ASA pour qu'il participe au routage dynamique.

Liaison de commande de grappe

Chaque nœud doit dédier une interface en tant qu'interface VXLAN (VTEP) pour la liaison de commande de grappe. Pour en savoir plus sur VXLAN, consultez Interfaces VXLAN, à la page 735.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP comporte deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier), et une interface normale appelée interface source du VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

Interface de la source VTEP

L'interface source du VTEP est une interface ASA virtuel classique à laquelle vous prévoyez associer l'interface VNI. Vous pouvez configurer une interface source de VTEP pour qu'elle agisse en tant que liaison de commande de grappe. L'interface source est réservée à une utilisation avec la liaison de commande de grappe uniquement. Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Interface VNI

Une interface VNI est semblable à une interface VLAN : il s'agit d'une interface virtuelle qui sépare le trafic réseau sur une interface physique donnée au moyen de balisage. Vous ne pouvez configurer qu'une seule interface VNI. Chaque interface VNI possède une adresse IP sur le même sous-réseau.

VTEP homologues

Contrairement au VXLAN habituel pour les interfaces de données, qui autorise un seul homologue VTEP, la mise en grappe ASA virtuel vous permet de configurer plusieurs homologues.

Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Échec de la liaison de commande de grappe

Si le protocole de liaison de commande de grappe tombe en panne pour une unité, la mise en grappe est désactivée; les interfaces de données sont fermées. Après avoir corrigé la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.



Remarque Lorsque l'ASA virtuel devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que l'unité a reçue du DHCP ou de l'ensemble d'adresses IP de la grappe. Si vous utilisez un ensemble d'adresses IP de grappe, si vous rechargez et que l'unité est toujours inactive dans la grappe, l'interface de gestion n'est pas accessible (car elle utilise alors l'adresse IP principale, qui est la même que le nœud de contrôle). Vous devez utiliser le port de console (si disponible) pour toute autre configuration.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

Gestion des grappes ASA virtuel

L'un des avantages de l'utilisation de la mise en grappe ASA virtuel est la facilité de gestion. Cette section décrit comment gérer la grappe.

Réseau de gestion

Nous vous conseillons de connecter tous les nœuds à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Interface de gestion

Utilisez l'interface Management 0/0 pour la gestion.

Remarque Vous ne pouvez pas activer le routage dynamique pour l'interface de gestion. Vous devez utiliser une route statique.

Vous pouvez utiliser l'adressage statique ou DHCP pour l'adresse IP de gestion.

Si vous utilisez l'adressage statique, vous pouvez utiliser l'adresse IP de la grappe principale qui est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle actuel. Pour chaque interface, vous configurez également une plage d'adresses de sorte que chaque nœud, y compris le nœud de contrôle actuel, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de gestion cohérent à une adresse; lorsqu'un nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente. L'adresse IP locale est utilisée pour le routage et est également utile pour la résolution de problèmes. Par exemple, vous pouvez gérer la grappe en vous connectant à l'adresse IP de la grappe principale, qui est toujours associée au nœud de contrôle actuel. Pour gérer un membre, vous pouvez vous connecter à l'adresse IP locale. Pour le trafic de gestion sortant tel que TFTP ou le journal système, chaque nœud, y compris le nœud de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Si vous utilisez DHCP, vous n'utilisez pas un ensemble d'adresses locales ou n'avez pas d'adresse IP de grappe principale.

Remarque Le trafic vers la boîte doit être acheminé vers l'adresse IP de gestion du nœud; le trafic vers la boîte n'est pas transféré sur la liaison de commande de grappe vers un autre nœud.

Gestion de nœud de contrôle vs Gestion de nœud de données

Toutes la gestion et la surveillance peuvent avoir lieu sur le nœud de contrôle. À partir du nœud de contrôle, vous pouvez vérifier les statistiques d'exécution, l'utilisation des ressources ou d'autres informations de

surveillance sur tous les nœuds. Vous pouvez également transmettre une commande à tous les nœuds de la grappe et reproduire les messages de console des nœuds de données vers le nœud de contrôle.

Vous pouvez surveiller directement les nœuds de données si vous le souhaitez. Bien que cela soit également disponible à partir du nœud de contrôle, vous pouvez effectuer la gestion de fichiers sur les nœuds de données (y compris la sauvegarde de la configuration et la mise à jour des images). Les fonctions suivantes ne sont pas disponibles à partir du nœud de commande :

- Surveillance des statistiques propres à la grappe par nœud.
- Surveillance des journaux système par nœud (sauf pour les journaux système envoyés à la console lorsque la duplication de la console est activée).
- SNMP
- NetFlow

duplication de clé de chiffrement

Lorsque vous créez une clé de chiffrement sur le nœud de contrôle, la clé est répliquée sur tous les nœuds de données. Si vous avez une session SSH sur l'adresse IP de la grappe principale, vous serez déconnecté en cas de défaillance du nœud de contrôle. Le nouveau nœud de contrôle utilise la même clé pour les connexions SSH, de sorte que vous n'avez pas besoin de mettre à jour la clé d'hôte SSH mise en cache lorsque vous vous reconnectez au nouveau nœud de contrôle.

Incompatibilité d'adresse IP du certificat de connexion ASDM

Par défaut, un certificat autosigné est utilisé pour la connexion ASDM en fonction de l'adresse IP locale. Si vous vous connectez à l'adresse IP de la grappe principale à l'aide d'ASDM, un message d'avertissement concernant une adresse IP non concordante peut s'afficher, car le certificat utilise l'adresse IP locale, et non l'adresse IP de la grappe principale. Vous pouvez ignorer le message et établir la connexion ASDM. Cependant, pour éviter ce type d'avertissement, vous pouvez inscrire un certificat qui contient l'adresse IP de la grappe principale et toutes les adresses IP locales de l'ensemble d'adresses IP. Vous pouvez ensuite utiliser ce certificat pour chaque membre de la grappe. Consultez https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html pour de plus amples renseignements.

Mise en grappe inter-sites

Pour les installations inter-sites, vous pouvez profiter de la mise en grappe d'ASA virtuel tant que vous suivez les lignes directrices recommandées.

Vous pouvez configurer chaque châssis de grappe pour qu'il appartienne à un ID de site distinct. Les ID de site sont utilisés pour permettre la mobilité de flux à l'aide de l'inspection LISP, la localisation du directeur pour améliorer les performances et réduire la latence aller-retour pour la mise en grappe inter-sites pour les centres de données, et la redondance des sites pour les connexions où un propriétaire de secours d'un flux se trouve toujours sur un autre site que celui du propriétaire.

Consultez les sections suivantes pour en savoir plus sur la mise en grappe inter-sites :

- Dimensionnement de l'interconnexion du centre de données : Exigences et conditions préalables à la mise en grappe d'ASA virtuel, à la page 552
- Lignes directrices inter-sites : Lignes directrices de la mise en grappe d'ASA virtuel, à la page 553
- Configurer la mobilité des flux de grappes : Configurer la mobilité des flux de grappes, à la page 576

- Activer la localisation du directeur : Activer la localisation du directeur, à la page 575
- Activer la redondance de site : Activer la localisation du directeur, à la page 575
- Exemples inter-sites : Exemple inter-sites nord-sud de mode routé d'interface individuelle, à la page 597

Licences pour la mise en grappe d'ASA virtuel

Chaque nœud de grappe nécessite la même licence de modèle. Nous vous conseillons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au membre le moins performant. Le niveau de débit sera répliqué du nœud de contrôle à chaque nœud de données afin qu'ils correspondent.

Remarque Si vous annulez l'enregistrement de l'ASA virtuel pour qu'il ne soit pas sous licence, il reviendra à un état de débit fortement limité si vous rechargez l'ASA virtuel. Un nœud de grappe sans licence et à faible performance aura une incidence négative sur les performances de l'ensemble de la grappe. Assurez-vous de conserver tous les nœuds de la grappe sous licence ou de supprimer les nœuds sans licence.

Exigences et conditions préalables à la mise en grappe d'ASA virtuel

Exigences du modèle

- ASAv30, ASAv50, ASAv100
- Les services en cloud privé suivants :
  - KVM
  - VMware
- Un maximum de 16 nœuds dans une grappe sur *deux* hôtes dans une configuration de déploiement 2 x 8. Nous vous conseillons de déployer un maximum de *huit* ASAv sur chacun des *deux* hôtes (2 x 8), ce qui donne une grappe de 16 nœuds.

Plateforme ASA virtuel et configuration logicielle requise

Tous les nœuds d'une grappe :

- Il doit s'agir du même modèle. Nous vous conseillons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au nœud le moins performant.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.

- Les nouveaux membres de la grappe doivent utiliser le même paramètre de chiffrement SSL (la commande **ssl encryption**) que le nœud de contrôle pour la communication de la liaison de commande de grappe initiale avant la réplication de la configuration.

Lignes directrices de la mise en grappe d'ASA virtuel

Basculement

Le basculement n'est pas pris en charge avec la mise en grappe.

IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, activation ou désactivation d'une interface sur l'ASA ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité de l'interface.
- Lors de l'ajout d'un nœud à une grappe existante ou lors du rechargement d'un nœud, il se produit une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Nous ne prenons pas en charge les VXLAN pour les interfaces de données; seule la liaison de commande de grappe prend en charge VXLAN.
- Il faut du temps pour répliquer les modifications sur toutes les unités d'une grappe. Si vous apportez une modification importante, par exemple, ajouter une règle de contrôle d'accès qui utilise des groupes d'objets (qui, lorsqu'ils sont déployés, sont divisés en plusieurs règles), le temps nécessaire pour effectuer la modification peut dépasser le délai d'expiration des nœuds de la grappe avec un message de réussite. Si cela se produit, vous pourriez voir le message « Échec de la réplication de la commande ». Vous pouvez ignorer le message.

Valeurs par défaut pour la mise en grappe d'ASA virtuel

- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Le rééquilibrage de la connexion est désactivé par défaut. Si vous activez le rééquilibrage de la connexion, l'intervalle par défaut entre les échanges d'informations de chargement est de 5 secondes.

• Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe d'ASA virtuel à l'aide d'une configuration Day0

Configuration Day0 du nœud de contrôle

La configuration Day0 suivante pour le nœud de contrôle comprend la configuration de démarrage suivie de la configuration d'interface qui sera répliquée sur les nœuds de données. Le texte en gras affiche les valeurs que vous devez modifier pour la configuration Day0 du nœud de données.

Remarque Cette configuration comprend uniquement la configuration centré sur la grappe. Votre configuration Day0 doit également inclure d'autres paramètres pour les licences, l'accès SSH , l'accès ASDM , etc. Consultez le guide de démarrage pour en savoir plus sur les configurations Day0.

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.51 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
```

```
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit A
cluster-interface vni1 ip 10.2.2.1 255.255.255.0
priority 1
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

Configuration Day0 du nœud de données

La configuration Day0 suivante pour le nœud de données inclut uniquement la configuration de démarrage. Le texte en gras affiche les valeurs que vous devez modifier à partir de la configuration Day0 du nœud de contrôle.

Remarque Cette configuration comprend uniquement la configuration centré sur la grappe. Votre configuration Day0 doit également inclure d'autres paramètres pour les licences, l'accès SSH , l'accès ASDM , etc. Consultez le guide de démarrage pour en savoir plus sur les configurations Day0.

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
```

```
network-object host 10.6.6.53
network-object host 10.6.6.54
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.52 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit B
cluster-interface vni1 ip 10.2.2.2 255.255.255.0
priority 2
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
```

```
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

Configurer la mise en grappe ASA virtuel après le déploiement

Pour configurer la mise en grappe après avoir déployé vos ASA virtuel, effectuez les tâches suivantes.

Configurer les paramètres d'interface

Configurez le mode d'interface de grappe sur chaque nœud ainsi que les interfaces sur le nœud de contrôle. La configuration d'interface sera répliquée sur les nœuds de données lorsqu'ils rejoignent la grappe. Notez que la configuration de la laision de commande de grappe est traitée dans la procédure de configuration de démarrage.

Configurer le mode d'interface de grappe de chaque nœud

Avant d'activer la mise en grappe, vous devez convertir le pare-feu pour utiliser des interfaces individuelles. Étant donné que la mise en grappe limite les types d'interfaces que vous pouvez utiliser, ce processus vous permet de vérifier votre configuration existante pour détecter les interfaces incompatibles, puis vous empêche de configurer des interfaces non prises en charge.

Avant de commencer

- Vous devez définir le mode séparément sur chaque ASA virtuel que vous souhaitez ajouter à la grappe.
- Connectez-vous à l'interface de ligne de commande de l'ASA virtuel en utilisant le port de console (si disponible) ou SSH (si configuré). Si aucune de ces options n'est disponible, vous pouvez utiliser ASDM pour configurer la mise en grappe.

Procédure

Étape 1 Affichez toute configuration incompatible afin de pouvoir forcer le mode d'interface et corriger votre configuration ultérieurement; le mode n'est pas modifié avec cette commande :

cluster interface-mode individual check-details

Exemple :

```
ciscoasa(config)# cluster interface-mode individual check-details
```

Mise en garde
Après avoir défini le mode d'interface, vous pouvez continuer à vous connecter à l'interface à l'aide de SSH; cependant, si vous rechargez l'ASA avant de configurer votre interface de gestion pour respecter les exigences de mise en grappe (par exemple, ajout d'un ensemble d'adresses IP de grappe ou obtention de l'adresse IP de DHCP), vous ne pourrez pas vous reconnecter, car la configuration d'interface incompatible avec la grappe

est supprimée. Dans ce cas, vous devrez vous connecter au port de console, si disponible, pour corriger la configuration d'interface.

Étape 2 Définissez le mode d'interface pour la mise en grappe :

cluster interface-mode individual force

Exemple :

```
ciscoasa(config)# cluster interface-mode individual force
```

Il n'y a pas de paramètres par défaut; vous devez choisir explicitement le mode. Si vous n'avez pas défini le mode, vous ne pouvez pas activer la mise en grappe.

L'option **force** change le mode sans vérifier si votre configuration comporte des paramètres incompatibles. Vous devez résoudre manuellement tous les problèmes de configuration après avoir changé de mode. Étant donné que toute configuration d'interface ne peut être corrigée qu'après avoir défini le mode, nous vous conseillons d'utiliser l'option **force** afin de pouvoir au moins partir de la configuration existante. Vous pouvez réexécuter l'option **check-details** après avoir défini le mode pour obtenir plus de conseils.

Sans l'option **force**, en cas de configuration incompatible, vous êtes invité à effacer votre configuration et à la recharger, ce qui vous obligera à vous connecter au port de console (si disponible) pour reconfigurer votre accès de gestion. Si votre configuration est compatible (ce qui est rare), le mode est modifié et la configuration est conservée. Si vous ne souhaitez pas effacer votre configuration, vous pouvez quitter la commande en tapant **n**.

Pour supprimer le mode d'interface, saisissez la commande **no cluster interface-mode**.

Configurer les interfaces individuelles

Vous devez modifier toute interface actuellement configurée avec une adresse IP pour qu'elle soit prête pour la grappe avant d'activer la mise en grappe. Au minimum, vous devrez peut-être modifier l'interface de gestion à laquelle SSH est actuellement connecté lorsque vous utilisez une adresse IP statique pour la gestion. Pour les autres interfaces, vous pouvez les configurer avant ou après avoir activé la mise en grappe; nous vous conseillons de préconfigurer toutes vos interfaces afin que la configuration complète soit synchronisée avec les nouveaux nœuds de la grappe.

Cette section décrit comment configurer les interfaces pour qu'elles soient compatibles avec la mise en grappe. Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre adresse IP prise dans un ensemble d'adresses IP. L'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle actuel. Toutes les interfaces de données doivent être des interfaces individuelles.

Pour l'interface de gestion, vous pouvez configurer un ensemble d'adresses IP ou utiliser le protocole DHCP; seule l'interface de gestion prend en charge l'obtention d'une adresse de DHCP. Pour utiliser DHCP, n'utilisez pas cette procédure; configurez-le plutôt comme d'habitude (voir Configurer les paramètres généraux de l'interface en mode routé, à la page 768).

Avant de commencer

- (Facultatif) Configurez les sous-interfaces.

- Pour l'interface de gestion, vous pouvez utiliser une adresse statique ou le protocole DHCP. Si vous utilisez des adresses IP statiques et que vous vous connectez à distance à l'interface de gestion à l'aide de SSH, l'adresse IP actuelle des nœuds de données potentiels est à usage temporaire.
  - Une adresse IP sera attribuée à chaque membre dans l'ensemble d'adresses IP de la grappe défini sur le nœud de contrôle.
  - L'ensemble d'adresses IP de la grappe ne peut pas inclure des adresses déjà utilisées sur le réseau, y compris de potentielles adresses IP secondaires.

    Par exemple :

    1. Vous configurez le nœud de contrôle pour qu'il utilise 10.1.1.1.
    2. Les autres nœuds utilisent 10.1.1.2, 10.1.1.3 et 10.1.1.4.
    3. Lorsque vous configurez l'ensemble d'adresses IP de la grappe sur le nœud de contrôle, vous ne pouvez pas inclure les adresses .2, .3 ou .4 dans l'ensemble, car elles sont déjà utilisées.
    4. Vous devez plutôt utiliser d'autres adresses IP sur le réseau, telles que .5, .6, .7 et .8.

Remarque L'ensemble a besoin d'autant d'adresses qu'il y a de membres dans la grappe, y compris le nœud de contrôle; l'adresse .1 d'origine est l'adresse IP principale de la grappe qui appartient au nœud de contrôle actuel.

    5. Après avoir rejoint la grappe, les anciennes adresses temporaires sont abandonnées et peuvent être utilisées ailleurs.

Procédure

Étape 1 Configurez un ensemble d'adresses IP locales (IPv4 et/ou IPv6), dont une sera affectée à chaque nœud de grappe pour l'interface :

(IPv4)

ip local pool *poolname first-address — last-address* [**mask** *mask*]

(IPv6)

ipv6 local pool *poolname ipv6-address*/*prefix-length number_of_addresses*

Exemple :

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8:45:1003/64 8
```

Incluez au moins autant d'adresses qu'il y a de nœuds dans la grappe. Si vous prévoyez d'étendre la grappe, incluez des adresses supplémentaires. L'adresse IP principale de la grappe qui appartient au nœud de contrôle actuel ne fait *pas* partie de cet ensemble; assurez-vous de réserver une adresse IP sur le même réseau pour l'adresse IP principale de la grappe.

Vous ne pouvez pas déterminer à l'avance l'adresse locale exacte attribuée à chaque nœud; pour voir l'adresse utilisée sur chaque nœud, saisissez la commande **show ip**[**v6**] **local pool** *poolname*. Chaque membre de la grappe se voit attribuer un ID de membre lorsqu'il rejoint la grappe. L'ID détermine l'adresse IP locale utilisée à partir de l'ensemble.

Étape 2 Entrez le mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/1
```

Étape 3 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif inside
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur.

Étape 4 Définissez l'adresse IP principale de la grappe et identifiez l'ensemble de grappes :

(IPv4)

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

(IPv6)

ipv6 address *ipv6-address*/*prefix-length* **cluster-pool** *poolname*

Exemple :

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8:45:1003::99/64 cluster-pool insipv6
```

Cette adresse IP doit être sur le même réseau que les adresses de l'ensemble d'adresses de la grappe, mais ne doit pas faire partie de ce dernier. Vous pouvez configurer une adresse IPv4 et/ou une adresse IPv6.

Les configurations automatiques DHCP, PPPoE et IPv6 ne sont pas prises en charge; vous devez configurer manuellement les adresses IP. La configuration manuelle de l'adresse Link-Local n'est pas non plus prise en charge.

Étape 5 Définissez le niveau de sécurité, où *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé) :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 100
```

Étape 6 Activez l'interface :

no shutdown

Exemples

L'exemple suivant configure les interfaces Management 0/0, GigabitEthernet 0/0 et GigabitEthernet 0/1 en tant qu'interfaces individuelles :

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface management 0/0
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8:45:1001::99/64 cluster-pool mgmtipv6
security-level 100
no shutdown

ip local pool out 209.165.200.225-209.165.200.232
ipv6 local pool outipv6 2001:DB8:45:1002/64 8

interface gigabitethernet 0/0
nameif outside
ip address 209.165.200.233 255.255.255.224 cluster-pool out
ipv6 address 2001:DB8:45:1002::99/64 cluster-pool outipv6
security-level 0
no shutdown

ip local pool ins 192.168.1.2-192.168.1.9
ipv6 local pool insipv6 2001:DB8:45:1003/64 8

interface gigabitethernet 0/1
nameif inside
ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ipv6 address 2001:DB8:45:1003::99/64 cluster-pool insipv6
security-level 100
no shutdown
```

Créer la configuration de démarrage

Chaque nœud de la grappe nécessite une configuration de démarrage pour rejoindre la grappe.

Configurer les paramètres de démarrage du nœud de contrôle

Chaque nœud de la grappe nécessite une configuration de démarrage pour rejoindre la grappe. En règle générale, le premier nœud que vous configurez pour rejoindre la grappe sera le nœud de contrôle. Après avoir activé la mise en grappe, après une période de sélection, la grappe choisit un nœud de contrôle. Avec un seul nœud dans la grappe au départ, ce nœud deviendra le nœud de contrôle. Les nœuds que vous ajouterez ensuite à la grappe seront des nœuds de données.

Avant de commencer

- Sauvegardez vos configurations au cas où vous souhaiteriez quitter la grappe ultérieurement et deviez restaurer votre configuration.

- À l'exception de la liaison de commande de grappe et de l'interface de gestion, qui peut éventuellement utiliser DHCP, toutes les interfaces de votre configuration doivent être configurées avec un ensemble d'adresses IP de grappe avant d'activer la mise en grappe. Si vous avez une configuration d'interface préexistante, vous pouvez soit effacer la configuration d'interface (**clear configure interface**), soit convertir vos interfaces en interfaces de grappe avant d'activer la mise en grappe.
- Lorsque vous ajoutez un nœud à une grappe en cours d'exécution, il se peut que vous constatiez des interruptions temporaires et limitées de paquets/connexions; c'est un comportement prévu.
- Activez la réservation de bâti grand format pour une utilisation avec la liaison de commande de grappe, afin de pouvoir définir la MTU de la liaison de commande de grappe à la valeur conseillée. Consultez la commande **jumbo-frame reservation**. L'activation des bâtis grand format entraîne le rechargement de l'ASA. Vous devez donc effectuer cette étape avant de poursuivre cette procédure.

Procédure

Étape 1 Configurez une interface VXLAN pour l'interface de liaison de commande de grappe avant de joindre la grappe.

Vous identifierez ultérieurement cette interface comme la liaison de commande de grappe lorsque vous activerez la mise en grappe.

La configuration de l'interface de liaison de commande de grappe n'est pas répliquée du nœud de contrôle aux nœuds de données; cependant, vous devez utiliser la même configuration sur chaque nœud. Comme cette configuration n'est pas répliquée, vous devez configurer les interfaces de liaison de commande de grappe séparément sur chaque nœud.

a) Identifiez les adresses IP homologues VTEP en créant un groupe d'objets réseau.

Consultez le chapitre « Objets pour le contrôle d'accès » du guide de configuration du pare-feu ASA pour en savoir plus sur les groupes d'objets réseau.

Le réseau IP sous-jacent entre les VTEP est indépendant du réseau de liaison de commande de grappe utilisé par les interfaces VNI. Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Exemple :

L'exemple suivant crée un groupe d'objets réseau avec des hôtes définis en ligne :

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
```

L'exemple suivant crée un groupe d'objets réseau qui fait référence à un objet réseau autonome :

```
ciscoasa(config)# object network xyz
ciscoasa(config-network-object)# range 10.6.6.51 10.6.6.54

ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object object xyz
```

b) Configurez l'interface source VTEP.

interface *interface_id*

nve-only cluster

nameif *name*

ip address *ip_address subnet_mask*

no shutdown

L'adresse IP doit être incluse comme l'un des homologues dans le groupe d'objets réseau.

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/7
ciscoasa(config-if)# nve-only cluster
ciscoasa(config-if)# nameif ccl
ciscoasa(config-if)# ip address 10.6.6.51 255.255.255.0
ciscoasa(config-if)# no shutdown
```

c) Associez l'interface source VTEP à l'instance NVE.

nve 1

source-interface *interface-name*

peer-group *network_object_name*

Vous ne pouvez spécifier qu'une seule instance NVE, avec l'ID 1.

La commande **encapsulation vxlan** est ajoutée par défaut pour l'instance NVE; vous n'avez pas besoin de l'ajouter explicitement.

Exemple :

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface ccl
ciscoasa(cfg-nve)# peer-group cluster-peers
```

d) Spécifiez l'unité de transfert maximale de l'interface source VTEP, qui doit être supérieure d'au moins 154 octets à la MTU la plus élevée des interfaces de données.

mtu *interface_name bytes*

Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets). Définissez la MTU entre 1 554 et 9 198 octets, , mais pas entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille MTU n'est pas optimale pour le fonctionnement du système. Par défaut, la MTU est de 1554 octets. Nous vous suggérons de définir la MTU de liaison de commande de grappe à 1 654 lorsque les interfaces de données sont fixées à 1 500; cette valeur nécessite la réservation de bâti grand format (voir la commande **jumbo-frame reservation**).

Par exemple, lors de l'utilisation d'un bâti grand format, comme la MTU maximale est de 9 198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9 044, tandis que la liaison de commande de grappe peut être définie sur 9 198.

Cette commande est répliquée sur les nœuds de données, mais nous vous conseillons de configurer ce paramètre avec les paramètres de démarrage.

Exemple :

```
ciscoasa(config)# mtu ccl 1654
```

e) (Facultatif) Définissez le port UDP VXLAN.

vxlan *port number*

Par défaut, l'interface source VTEP accepte le trafic VXLAN vers le port UDP 4789. Si votre réseau utilise un port non standard, vous pouvez le modifier.

Exemple :

```
ciscoasa(config)# vxlan port 5678
```

f) Créez l'interface VNI.

interface vni *vni_num*

segment-id *ID*

vtep-nve 1

Exemple :

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
```

- Définissez le numéro VNI entre 1 et 10 000. Cet ID est uniquement un identifiant d'interface interne.
- Définissez l'ID de segment entre 1 et 16777215. L'ID de segment est utilisé pour le balisage VXLAN.

Ne configurez *pas* de nom pour l'interface ni d'autres paramètres.

Étape 2 Nommez la grappe et passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Le nom doit être une chaîne ASCII comptant de 1 à 38 caractères. Vous ne pouvez configurer qu'un seul groupe de grappes par nœud. Tous les membres de la grappe doivent utiliser le même nom.

Étape 3 Nommez ce membre de la grappe :

local-unit *node_name*

Utilisez une chaîne ASCII unique de 1 à 38 caractères. Chaque nœud doit avoir un nom unique. Un nœud ayant un nom en double ne sera pas autorisé dans la grappe.

Exemple :

```
ciscoasa(cfg-cluster)# local-unit node1
```

Étape 4 Spécifiez l'interface VNI de la liaison de commande de grappe :

cluster-interface *vni_interface_id* **ip** *ip_address mask*

Exemple :

```
ciscoasa(cfg-cluster)# cluster-interface vni1 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on VNI1
```

Spécifiez une adresse IPv4 pour l'adresse IP; IPv6 n'est pas pris en charge pour cette interface. Pour chaque nœud, spécifiez une adresse IP différente sur le même réseau. Le réseau VNI est le réseau virtuel chiffré qui s'exécute sur le réseau physique VTEP.

Étape 5 Définissez la priorité de ce nœud pour les sélections de nœud de contrôle :

priority *priority_number*

Exemple :

```
ciscoasa(cfg-cluster)# priority 1
```

La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée.

Étape 6 (Facultatif) Définissez une clé d'authentification pour le trafic de contrôle sur la liaison de commande de grappe :

key *shared_secret*

Exemple :

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le code secret partagé est utilisé pour générer la clé de chiffrement. Cette commande n'influe pas sur le trafic du chemin de données, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair.

Étape 7 Activez la mise en grappe :

enable [**noconfirm**]

Exemple :

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
```

```
INFO: Done
```

Lorsque vous saisissez la commande **enable**, l'ASA analyse la configuration en cours d'exécution à la recherche de commandes incompatibles, en vue de cerner des fonctionnalités qui ne sont pas prises en charge avec la grappe, y compris les commandes pouvant être présentes dans la configuration par défaut. Vous êtes invité à supprimer les commandes incompatibles. Si vous répondez **No** (Non), la mise en grappe n'est pas activée. Utilisez le mot clé **noconfirm** pour contourner la confirmation et supprimer automatiquement les commandes incompatibles.

Pour le premier nœud activé, une sélection de nœud de contrôle se produit. Comme le premier nœud doit être le seul membre de la grappe jusqu'à présent, il deviendra le nœud de contrôle. N'effectuez aucune modification de configuration pendant cette période.

Pour désactiver la mise en grappe, saisissez la commande **no enable**.

Remarque
Si vous désactivez la mise en grappe, toutes les interfaces de données sont fermées et seule l'interface de gestion est active.

Exemples

L'exemple suivant configure les interfaces de gestion, interne et externe et la liaison de commande de grappe VXLAN, puis active la mise en grappe pour l'ASA appelé « node1 », qui deviendra le nœud de contrôle parce qu'il sera ajouté en premier à la grappe :

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8:45:1001::99/64 cluster-pool mgmtipv6
    security-level 100
    no shutdown

ip local pool out 209.165.200.225-209.165.200.232
ipv6 local pool outipv6 2001:DB8:45:1002/64 8

interface gigabitethernet 0/0
    nameif outside
    ip address 209.165.200.233 255.255.255.224 cluster-pool out
    ipv6 address 2001:DB8:45:1002::99/64 cluster-pool outipv6
    security-level 0
    no shutdown

ip local pool ins 192.168.1.2-192.168.1.9
ipv6 local pool insipv6 2001:DB8:45:1003/64 8

interface gigabitethernet 0/1
    nameif inside
    ip address 192.168.1.1 255.255.255.0 cluster-pool ins
    ipv6 address 2001:DB8:45:1003::99/64 cluster-pool insipv6
    security-level 100
    no shutdown

object-group network cluster-peers
```

```
    network-object host 10.6.6.51
    network-object host 10.6.6.52
    network-object host 10.6.6.53
    network-object host 10.6.6.54

interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
    ip address 10.6.6.51 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

mtu ccl 1654

interface vni 1
    segment-id 1000
    vtep-nve 1

cluster group pod1
    local-unit node1
    cluster-interface vni1 ip 192.168.1.1 255.255.255.0
    priority 1
    key 67impala
    enable noconfirm
```

Configurer les paramètres de démarrage du nœud de données

Exécutez la procédure suivante pour configurer les nœuds de données.

Avant de commencer

- Sauvegardez vos configurations au cas où vous souhaiteriez quitter la grappe ultérieurement et deviez restaurer votre configuration.
- À l'exception de la liaison de commande de grappe et de l'interface de gestion, qui peut éventuellement utiliser DHCP, toutes les interfaces de votre configuration doivent être configurées avec un ensemble d'adresses IP de grappe avant d'activer la mise en grappe. Si vous avez une configuration d'interface préexistante, vous pouvez soit effacer la configuration d'interface (**clear configure interface**), soit convertir vos interfaces en interfaces de grappe avant d'activer la mise en grappe.
- Lorsque vous ajoutez un nœud à une grappe en cours d'exécution, il se peut que vous constatiez des interruptions temporaires et limitées de paquets/connexions; c'est un comportement prévu.
- Activez la réservation de bâti grand format pour une utilisation avec la liaison de commande de grappe, afin de pouvoir définir la MTU de la liaison de commande de grappe à la valeur conseillée. Consultez la commande **jumbo-frame reservation**. L'activation des bâtis grand format entraîne le rechargement de l'ASA. Vous devez donc effectuer cette étape avant de poursuivre cette procédure.

Procédure

Étape 1 Configurez la même interface de liaison de commande de grappe que celle que vous avez configurée pour le nœud de contrôle. Assurez-vous de fournir une adresse IP différente pour l'interface source VTEP (indiquée en **gras**).

Exemple :

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
ciscoasa(config)# interface gigabitethernet 0/7
ciscoasa(config-if)# nve-only cluster
ciscoasa(config-if)# nameif ccl
ciscoasa(config-if)# ip address 10.6.6.52 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface ccl
ciscoasa(cfg-nve)# peer-group cluster-peers
ciscoasa(config)# mtu ccl 1654
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
```

Étape 2 Saisissez le même nom de grappe que celui que vous avez configuré pour le nœud de contrôle :

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 3 Nommez ce membre de la grappe avec une chaîne unique :

local-unit *node_name*

Exemple :

```
ciscoasa(cfg-cluster)# local-unit node2
```

Spécifiez une chaîne ASCII de 1 à 38 caractères.

Chaque nœud doit avoir un nom unique. Un nœud ayant un nom en double ne sera pas autorisé dans la grappe.

Étape 4 Spécifiez la même interface de liaison de commande de grappe que vous avez configurée pour le nœud de contrôle, mais spécifiez une adresse IP différente sur le même réseau pour chaque nœud :

cluster-interface *vni_interface_id* **ip** *ip_address mask*

Exemple :

```
ciscoasa(cfg-cluster)# cluster-interface vni1 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on VNI1
```

Spécifiez une adresse IPv4 pour l'adresse IP; IPv6 n'est pas pris en charge pour cette interface. Cette interface ne peut pas avoir de **nameif** configuré.

Étape 5 Si vous utilisez la mise en grappe inter-sites, définissez l'ID de site pour ce nœud afin qu'il utilise une adresse MAC spécifique au site :

site-id *number*

Exemple :

```
ciscoasa(cfg-cluster)# site-id 2
```

Le **number** est compris entre 1 et 8.

Étape 6 Définissez la priorité de ce nœud pour les sélections de nœuds de contrôle, généralement à une valeur plus élevée que celle du nœud de contrôle :

priority *priority_number*

Exemple :

```
ciscoasa(cfg-cluster)# priority 2
```

Définissez la priorité entre 1 et 100, 1 représentant la priorité la plus élevée.

Étape 7 Définissez la même clé d'authentification que vous avez définie pour le nœud de contrôle :

Exemple :

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

Étape 8 Activez la mise en grappe :

enable as-data-node

Vous pouvez éviter toute incompatibilité de configuration (principalement l'existence d'interfaces non encore configurées pour la mise en grappe) en utilisant la commande **enable as-data-node**. Cette commande garantit que le nœud de données rejoint la grappe sans possibilité de devenir le nœud de contrôle dans une sélection actuelle. Sa configuration est remplacée par celle synchronisée à partir du nœud de contrôle.

Pour désactiver la mise en grappe, saisissez la commande **no enable**.

Remarque
Si vous désactivez la mise en grappe, toutes les interfaces de données sont fermées et seule l'interface de gestion est active.

Exemples

L'exemple suivant comprend la configuration d'un nœud de données, le nœud2 :

```
object-group network cluster-peers
    network-object host 10.6.6.51
    network-object host 10.6.6.52
```

```
    network-object host 10.6.6.53
    network-object host 10.6.6.54

interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
    ip address 10.6.6.52 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

mtu ccl 1654

interface vni 1
    segment-id 1000
    vtep-nve 1

cluster group pod1
    local-unit node2
    cluster-interface vni1 ip 192.168.1.2 255.255.255.0
    priority 2
    key 67impala
    enable noconfirm
```

Personnaliser l'opération de mise en grappe

Vous pouvez personnaliser la surveillance de l'intégrité de la mise en grappe, le délai de réplication de la connexion TCP, la mobilité des flux et d'autres optimisations, dans le cadre de la configuration day0 ou après le déploiement de la grappe.

Exécutez ces procédures sur le nœud de contrôle.

Configurer les paramètres de grappe ASA de base

Vous pouvez personnaliser les paramètres de grappe sur le nœud de contrôle.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Étape 2 (Facultatif) Activez la réplication de la console des nœuds de données vers le nœud de contrôle :

console-replicate

Par défaut, cette fonction est désactivée. L'ASA imprime certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de la console, les nœuds de données envoient les messages de la console au nœud de contrôle de sorte que vous ne devez surveiller qu'un seul port de console pour la grappe.

Étape 3 Définissez le niveau de trace minimal pour les événements de mise en grappe :

trace-level *level*

Définissez le niveau minimum comme souhaité :

- **critical**—Événements critiques (gravité=1)
- **warning**—Avertissements (gravité=2)
- **informational**—Événements informationnels (gravité=3)
- **debug**—Événements de débogage (gravité= 4)

Configurer les paramètres de surveillance de l'intégrité et de jonction automatique

Cette procédure permet de configurer la surveillance de l'intégrité des nœuds et des interfaces.

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Entrez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

Étape 2 Personnalisez la fonctionnalité de contrôle de l'intégrité des nœuds de la grappe.

health-check [**holdtime** *timeout*]

Pour déterminer l'intégrité des nœuds, les nœuds de la grappe ASA envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.

- **holdtime** *timeout* : détermine l'intervalle de temps entre les messages d'état de pulsation des nœuds, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver la fonctionnalité de contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées (**no health-check monitor-interface**). Lorsque la modification de la topologie est terminée et que la

modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver le contrôle d'intégrité.

Exemple :

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

Étape 3 Désactivez le contrôle d'intégrité de l'interface sur une interface.

no health-check monitor-interface *interface_id*

La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Le délai avant la suppression par l'ASA d'un membre de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces. Vous pouvez le désactiver pour chaque interface en utilisant la forme **no** (non) de cette commande. Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion.

- *interface_id* : désactive la supervision d'une interface. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver la fonctionnalité de contrôle d'intégrité (**no health-check**) et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver le contrôle d'intégrité.

Exemple :

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

Étape 4 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system** : spécifie les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.
- **unlimited** : (Par défaut pour le **cluster-interface**) Ne limite pas le nombre de tentatives de jonction.
- *auto-rejoin-max* : définit le nombre de tentatives de jonction, entre 0 et 65535. **0** désactive la jonction automatique. La valeur par défaut pour les commandes **data-interface** et **system** est de 3.
- *auto_rejoin_interval* : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- *auto_rejoin_interval_variation* : définit si la durée de l'intervalle augmente. Définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données et le système.

Exemple :

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

Étape 5 Configurez le délai antirebond avant que l'ASA considère une interface comme défaillante et que le nœud ne soit supprimé de la grappe.

health-check monitor-interface debounce-time *ms*

Exemple :

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

Définissez le délai antirebond entre 300 et 9 000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe.

Étape 6 (Facultatif) Configurez la surveillance de la charge de trafic.

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* : définit le délai en secondes entre les messages de surveillance, entre 10 et 360 secondes. La valeur par défaut est de 20 secondes.
- **intervals** *intervals* : définit le nombre d'intervalles pour lesquels l'ASA conserve les données, entre 1 et 60. La valeur par défaut est 30.

Vous pouvez superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud si les nœuds restants peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Vous pouvez superviser périodiquement la charge de trafic. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud.

Utilisez la commande **show cluster info load-monitor** pour afficher la charge de trafic.

Exemple :

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

Exemple

L'exemple suivant configure le délai de rétention du contrôle d'intégrité à 0,3 seconde; désactive la surveillance sur l'interface Management 0/0; définit la reconnexion automatique pour les interfaces de données à 4 tentatives commençant à 2 minutes, en multipliant la durée de 3 fois l'intervalle précédent; et définit la reconnexion automatique pour la liaison de commande de grappe à 6 tentatives toutes les 2 minutes.

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

Configurer la rééquilibrage de la connexion et le délai de réplication TCP de la grappe

Vous pouvez configurer le rééquilibrage des connexions. Si les capacités d'équilibrage de charges des routeurs en amont ou en aval entraînent une répartition non équilibrée des flux, vous pouvez configurer des nœuds surchargés pour rediriger les nouveaux flux TCP vers d'autres nœuds. Aucun flux existant ne sera déplacé vers d'autres nœuds.

Activez le délai de réplication de la grappe pour les connexions TCP pour aider à éliminer le « travail inutile » lié aux flux de courte durée en retardant la création du flux directeur/de sauvegarde. Notez que si un nœud tombe en panne avant la création du flux directeur/de sauvegarde, ces flux ne peuvent pas être récupérés. De même, si le trafic est rééquilibré vers un autre nœud avant la création du flux, le flux ne peut pas être récupéré. Vous ne devez pas activer la réplication TCP pour le trafic sur lequel vous désactivez la répartition aléatoire TCP.

Procédure

Étape 1 Activez le délai de réplication de la grappe pour les connexions TCP :

cluster replication delay *seconds* {**http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] {**host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

Exemple :

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

Définissez les *secondes* entre 1 et 15. Le délai **http** est activé par défaut pendant 5 secondes.

Étape 2 Entrez en mode de configuration de la grappe :

cluster group *name*

Étape 3 (Facultatif) Activez le rééquilibrage des connexions pour le trafic TCP :

conn-rebalance [**frequency** *seconds*]

Exemple :

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

Cette commande est désactivée par défaut. Si cette option est activée, les ASA échangent périodiquement des renseignements sur les connexions par seconde et déchargent les nouvelles connexions des appareils ayant plus de connexions par seconde vers les appareils moins chargés. Les connexions existantes ne sont jamais déplacées. De plus, comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées. La valeur par défaut est de 5 secondes.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Configurer les fonctionnalités inter-sites

Pour la mise en grappe inter-sites, vous pouvez personnaliser votre configuration pour améliorer la redondance et la stabilité.

Activer la localisation du directeur

Pour améliorer les performances et réduire la latence d'aller-retour dans le cas de la mise en grappe inter-sites pour les centres de données, vous pouvez activer la localisation du directeur. Les nouvelles connexions sont généralement équilibrées et appartiennent aux membres de la grappe d'un site donné. Cependant, l'ASA attribue le rôle de directeur à un membre sur *n'importe quel* site. La localisation du directeur permet des rôles de directeur supplémentaires : un directeur local sur le même site que le propriétaire et un directeur global qui peut se trouver sur n'importe quel site. Le fait de maintenir le propriétaire et le directeur sur le même site améliore les performances. En cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site. Le directeur global est utilisé si un membre d'une grappe reçoit des paquets pour une connexion appartenant à un autre site.

Avant de commencer

- Définissez l'ID de site pour le membre de la grappe dans la configuration de démarrage.
- Les types de trafic suivants ne prennent pas en charge la localisation : trafic NAT ou PAT; trafic inspecté par SCTP; requête du propriétaire de la fragmentation.

Procédure

Étape 1 Entrez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

Étape 2 Activez la localisation du directeur.

director-localization

Activer la redondance de site

Pour protéger les flux contre une défaillance de site, vous pouvez activer la redondance de site. Si le propriétaire de connexion de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site.

Avant de commencer

- Définissez l'ID de site pour le membre de la grappe dans la configuration de démarrage.

Procédure

Étape 1 Entrez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

Étape 2 Activez la redondance de site.

site-redundancy

Configurer la mobilité des flux de grappes

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

À propos de l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux entre les sites.

À propos de LISP

La mobilité des machines virtuelles de centres de données, comme VMware VMotion, permet aux serveurs de migrer entre les centres de données tout en maintenant les connexions avec les clients. Pour prendre en charge une telle mobilité de serveur de centre de données, les routeurs doivent être en mesure de mettre à jour la route d'entrée vers le serveur lorsqu'il se déplace. L'architecture Cisco Locator/Protocole de séparation

d'ID (LISP) sépare l'identité du périphérique, ou l'identifiant de terminal (EID), de son emplacement, ou localisateur de routage, dans deux espaces de numérotation différents, ce qui rend la migration du serveur transparente pour les clients. Par exemple, lorsqu'un serveur est déplacé vers un nouveau site et qu'un client envoie du trafic vers le serveur, le routeur redirige le trafic vers le nouvel emplacement.

LISP nécessite des routeurs et des serveurs dans certains rôles, tels que le routeur de tunnel de sortie (ETR) LISP, le routeur de tunnel d'entrée (ITR), les routeurs de premier saut, le résolveur de carte (MR) et le serveur de carte (MS). Lorsque le routeur du premier saut du serveur détecte que le serveur est connecté à un autre routeur, il met à jour tous les autres routeurs et les bases de données afin que l'ITR connectée au client puisse intercepter, encapsuler et envoyer le trafic vers le nouvel emplacement du serveur.

Prise en charge du LISP ASA

L'ASA n'exécute pas le LISP lui-même; il peut, cependant, inspecter le trafic LISP pour détecter les changements d'emplacement, puis utiliser ces informations pour un fonctionnement de mise en grappe transparent. Sans l'intégration du LISP, lorsqu'un serveur est déplacé vers un nouveau site, le trafic est acheminé vers un membre de la grappe ASA sur le nouveau site plutôt que vers le propriétaire d'origine du flux. Le nouvel ASA transfère le trafic vers l'ASA au niveau de l'ancien site, puis l'ancien ASA doit renvoyer le trafic vers le nouveau site pour qu'il atteigne le serveur. Ce flux de trafic est sous-optimal et est connu comme « tromboning » ou « épingle à cheveux ».

Grâce à l'intégration du LISP, les membres de la grappe ASA peuvent inspecter le trafic LISP passant entre le routeur du premier saut et l'ETR ou l'ITR, puis peuvent changer le propriétaire du flux pour qu'il se trouve sur le nouveau site.

Lignes directrices LISP

- Les membres de la grappe ASA doivent se trouver entre le routeur du premier saut et l'ITR ou l'ETR du site. La grappe ASA elle-même ne peut pas être le premier routeur de saut pour un segment étendu.
- Seuls les flux entièrement distribués sont pris en charge; les flux centralisés, les flux semi-distribués ou les flux appartenant à des nœuds individuels ne sont pas transférés vers de nouveaux propriétaires. Les flux semi-distribués comprennent des applications, telles que SIP, où tous les flux enfants appartiennent au même ASA qui possède le flux parent.
- La grappe déplace uniquement les états de flux de couche 3 et 4; certaines données d'application pourraient être perdues.
- Pour les flux de courte durée ou non essentiels pour l'entreprise, le déplacement du propriétaire peut ne pas valoir la peine. Vous pouvez contrôler les types de trafic pris en charge avec cette fonctionnalité lorsque vous configurez la politique d'inspection. Vous devez limiter la mobilité de flux au trafic essentiel.

Mise en œuvre du LISP ASA

Cette fonctionnalité comprend plusieurs configurations interdépendantes (qui sont toutes décrites dans ce chapitre) :

1. (Facultatif) Limiter les EID inspectés en fonction de l'adresse IP de l'hôte ou du serveur : le routeur de premier saut pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée, vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.
2. Inspection du trafic LISP : l'ASA inspecte le trafic LISP sur le port UDP 4342 pour détecter le message EID-notify envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui

met en corrélation l'EID et l'ID de site. Par exemple, vous devez inspecter le trafic LISP avec une adresse IP source du routeur du premier saut et une adresse de destination de l'ITR ou de l'ETR. Remarque : le trafic LISP n'a pas de directeur affecté et le trafic LISP en lui-même ne participe pas au partage de l'état de la grappe.

3. Politique de service pour activer la mobilité des flux sur le trafic spécifié : vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.
4. ID de sites : l'ASA utilise l'ID de site pour chaque nœud de la grappe afin de déterminer le nouveau propriétaire.
5. Configuration au niveau de la grappe pour activer la mobilité de flux : vous devez également activer la mobilité de flux au niveau de la grappe. Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité de flux pour une classe particulière de trafic ou d'applications.

Configurer l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

Avant de commencer

- Affectez chaque unité de grappe à un ID de site en fonction de Configurer les paramètres de démarrage du nœud de contrôle, à la page 561 et Configurer les paramètres de démarrage du nœud de données, à la page 567.
- Le trafic LISP n'est pas inclus dans la classe de trafic d'inspection par défaut. Vous devez donc configurer une classe distincte pour le trafic LISP dans le cadre de cette procédure.

Procédure

Étape 1 (Facultatif) Configurez une carte d'inspection LISP pour limiter les EID inspectés en fonction de l'adresse IP et pour configurer la clé partagée LISP :

a) Créez une ACL étendue; seule l'adresse IP de destination correspond à l'adresse intégrée de l'EID :

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

Les ACL IPv4 et IPv6 sont acceptées. Consultez la référence de commande pour connaître la syntaxe **access-list extended** exacte.

b) Créez la carte d'inspection LISP et entrez le mode des paramètres :

policy-map type inspect lisp *inspect_map_name*

parameters

c) Définissez les EID autorisés en identifiant l'ACL que vous avez créée :

allowed-eid access-list *eid_acl_name*

Le routeur de premier saut ou l'ITR/ETR pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée; vous pouvez donc limiter les EID

à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.

d) Si nécessaire, saisissez la clé partagée :

validate-key *key*

Exemple :

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

Étape 2 Configurez l'inspection LISP pour le trafic UDP entre le routeur de premier saut et l'ITR ou l'ETR sur le port 4342 :

a) Configurez l'ACL étendue pour identifier le trafic LISP :

access list *inspect_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

Vous *devez* spécifier le port UDP 4342. Les ACL IPv4 et IPv6 sont acceptées. Consultez la référence de commande pour connaître la syntaxe **access-list extended** exacte.

b) Créez une carte de trafic pour l'ACL :

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) Spécifiez la liste des politiques, la carte de trafic, activez l'inspection à l'aide de la carte d'inspection LISP facultative et appliquez la politique de service à une interface (si nouvelle) :

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

Si vous avez une politique de service existante, spécifiez le nom de la liste des politiques existante. Par défaut, l'ASA inlcut une politique globale appelée **global_policy**, donc pour une politique globale, spécifiez ce nom. Vous pouvez également créer une politique de service par interface si vous ne souhaitez pas appliquer la politique à l'échelle mondiale. L'inspection LISP est appliquée au trafic de manière bidirectionnelle, vous n'avez donc pas besoin d'appliquer la politique de service sur les interfaces source et de destination; tout le trafic qui entre ou sort de l'interface à laquelle vous appliquez la liste des politiques est affecté si le trafic correspond à la carte de trafic dans les deux sens.

Exemple :

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
```

```
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

L'ASA inspecte le trafic LISP pour détecter le message de notification d'EID envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui met en corrélation l'EID et l'ID de site.

Étape 3 Activez la mobilité des flux pour une classe de trafic :

a) Configurez l'ACL étendue pour identifier le trafic opérationnel critique que vous souhaitez réaffecter au site le plus optimal lorsque les serveurs changent de site :

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

Les ACL IPv4 et IPv6 sont acceptées. Consultez la référence de commande pour connaître la syntaxe **access-list extended** exacte. Vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.

b) Créez une carte de trafic pour l'ACL :

class-map *flow_map_name*

match access-list *flow_acl_name*

c) Spécifiez la même liste des politiques sur laquelle vous avez activé l'inspection LISP, la carte de trafic de flux, et activez la mobilité des flux :

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

Exemple :

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

Étape 4 Entrez dans le mode de configuration du groupe de grappes et activez la mobilité des flux pour la grappe :

cluster group *name*

flow-mobility lisp

Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité des flux.

Exemples

L'exemple suivant :

- Limite les EID à ceux sur le réseau 10.10.10.0/24

- Inspecte le trafic LISP (UDP 4342) entre un routeur LISP à l'adresse 192.168.50.89 (à l'intérieur) et un routeur ITR ou ETTR (sur une autre interface ASA) à l'adresse 192.168.10.8
- Active la mobilité des flux pour tout le trafic interne vers un serveur sur 10.10.10.0/24 à l'aide de HTTPS.
- Active la mobilité des flux pour la grappe.

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

Gérer les nœuds de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les nœuds de cette dernière.

Devenir un nœud inactif

Pour devenir un membre inactif de la grappe, désactivez la mise en grappe sur le nœud tout en laissant intacte la configuration de mise en grappe.



Remarque Lorsqu'un ASA devient inactif (soit manuellement, soit à la suite d'un échec du contrôle d'intégrité), toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe; ou vous pouvez supprimer complètement le nœud de la grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), alors l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 2 Désactivez la mise en grappe :

no enable

Si ce nœud était le nœud de contrôle, une nouvelle sélection de contrôle a lieu et un autre membre devient le nœud de contrôle.

La configuration de la grappe est conservée, vous pouvez donc réactiver la mise en grappe ultérieurement.

Désactiver un nœud de données à partir du nœud de contrôle

Pour désactiver un membre autre que le nœud auquel vous êtes connecté, effectuez les étapes suivantes.



Remarque Lorsqu'un ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Procédure

Supprimez le nœud de la grappe.

cluster remove unit *node_name*

La configuration de démarrage reste inchangée, ainsi que la dernière configuration synchronisée à partir du nœud de contrôle, afin que vous puissiez rajouter le nœud ultérieurement sans perdre votre configuration. Si vous saisissez cette commande sur un nœud de données pour supprimer le nœud de contrôle, un nouveau nœud de contrôle est élu.

Pour afficher les noms des membres, saisissez **cluster remove unit ?**, ou saisissez la commande **show cluster info**.

Exemple :

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement un membre, vous devez rejoindre manuellement la grappe.

Procédure

Étape 1 Sur la console, passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 2 Activez la mise en grappe.

enable

Quitter la grappe

Si vous souhaitez quitter complètement la grappe, vous devez supprimer toute la configuration de démarrage de la grappe. Étant donné que la configuration actuelle sur chaque nœud est la même (synchronisée à partir de l'unité active), quitter la grappe implique également de restaurer une configuration antérieure à la grappe à partir d'une sauvegarde ou d'effacer votre configuration et de recommencer pour éviter les conflits d'adresses IP.

Procédure

Étape 1 Pour un nœud de données, désactivez la mise en grappe :

cluster group *cluster_name* **no enable**

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

Vous ne pouvez pas modifier la configuration lorsque la mise en grappe est activée sur un nœud de données.

Étape 2 Effacez la configuration de la grappe :

clear configure cluster

L'ASA désactive toutes les interfaces, y compris l'interface de gestion et la liaison de commande de grappe.

Étape 3 Désactivez le mode d'interface de la grappe :

no cluster interface-mode

Le mode n'est pas stocké dans la configuration et doit être réinitialisé manuellement.

Étape 4 Si vous avez une configuration de sauvegarde, copiez-la dans la configuration en cours d'exécution :

copy *backup_cfg* **running-config**

Exemple :

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

Étape 5 Enregistrez la configuration pour le démarrage :

write memory

Étape 6 Si vous n'avez pas de configuration de sauvegarde, reconfigurez l'accès de gestion. Par exemple, assurez-vous de modifier les adresses IP de l'interface et de restaurer le bon nom d'hôte.

Modifier le nœud de contrôle



Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez spécifier le nœud exact que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez toutefois que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle à l'aide de cette procédure, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Procédure

Définissez un nouveau nœud comme nœud de contrôle :

cluster control-node unit*node_name*

Exemple :

```
ciscoasa(config)# cluster control-node unit asa2
```

Vous devrez vous reconnecter à l'adresse IP de la grappe principale.

Pour afficher les noms des membres, saisissez **cluster control-node unit ?** (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exécuter une commande à l'échelle de la grappe

Pour envoyer une commande à tous les nœuds de la grappe ou à un nœud en particulier, procédez comme suit. L'envoi d'une commande **show** à tous les nœuds collecte toutes les sorties et les affiche sur la console du nœud actuel. D'autres commandes, telles que **capture** et **copy**, peuvent également profiter d'une exécution à l'échelle de la grappe.

Procédure

Envoyez une commande à tous les nœuds ou, si vous spécifiez le nom du nœud, à un nœud en particulier :

cluster exec [**unit** *node_name*] *command*

Exemple :

```
ciscoasa# cluster exec show xlate
```

Pour afficher les noms de nœud, saisissez **cluster exec unit ?** (unité d'exécution de grappe?) (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exemples

Pour copier simultanément le même fichier de capture de tous les nœuds de la grappe vers un serveur TFTP, saisissez la commande suivante sur le nœud de contrôle :

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Plusieurs fichiers PCAP, un pour chaque nœud, sont copiés sur le serveur TFTP. Le nom du fichier de capture de destination est automatiquement associé au nom du nœud, par exemple

capture1_asa1.pcap, capture1_asa2.pcap, etc. Dans cet exemple, asa1 et asa2 sont des noms de nœuds de grappe.

Supervision de la grappe ASA virtuel

Vous pouvez superviser et dépanner l'état de la grappe et les connexions.

Supervision de l'état de la grappe

Consultez les commandes suivantes pour superviser l'état de la grappe :

- **show cluster info** [**health** [**details**]]

  En l'absence de mot clé, la commande **show cluster info** affiche l'état de tous les membres de la grappe.

  La commande **show cluster info health** affiche l'intégrité actuelle des interfaces, des nœuds et de la grappe dans son ensemble. Le mot clé **details** affiche le nombre d'échecs de messages de pulsation.

  Consultez la sortie suivante pour la commande **show cluster info** :

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state CONTROL_NODE
      ID        : 2
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state DATA_NODE
      ID        : 3
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
```

```
    Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  Indique si le nœud de la grappe rejoindra automatiquement la grappe après un délai et si les conditions de défaillance (comme l'attente de la licence, l'échec de la vérification de l'intégrité du châssis, etc.) sont supprimées. Si le nœud est désactivé de façon permanente ou si le nœud est déjà dans la grappe, cette commande n'affichera aucune sortie.

  Consultez les sorties suivantes pour la commande **show cluster info auto-join** :

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport** {**asp** | **cp** [**detail**]}

  Affiche les statistiques relatives au transport pour les éléments suivants :

  - **asp** – Statistiques de transport du plan de données.
  - **cp** – Statistiques de transport du plan de commande.

    Si vous saisissez le mot clé **detail**, vous pouvez afficher l'utilisation du protocole de transport fiable de la grappe afin de cerner les problèmes d'abandon de paquet lorsque le tampon est plein dans le plan de commande. Consultez la sortie suivante pour la commande **show cluster info transport cp detail** :

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
```

```
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0
```

```
    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  -----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  -----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  -----------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                         578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
```

```
=============================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  Affiche l'historique de la grappe, ainsi que les messages d'erreur indiquant pourquoi un nœud de grappe n'a pas pu se joindre ou pourquoi un nœud a quitté a grappe.

Capture des paquets à l'échelle de la grappe

Consultez la commande suivante pour capturer des paquets dans une grappe :

cluster exec capture

Pour prendre en charge le dépannage à l'échelle de la grappe, vous pouvez activer la capture du trafic spécifique à la grappe sur le nœud de contrôle à l'aide de la commande **cluster exec capture**, qui est ensuite automatiquement activée sur tous les nœuds de données de la grappe.

Supervision des ressources de la grappe

Consultez la commande suivante pour surveiller les ressources de la grappe :

show cluster {**cpu** | **memory** | **resource**} [*options*]

Affiche les données agrégées pour l'ensemble de la grappe. Les *options* disponibles dépendent du type de données.

Supervision du trafic de la grappe

Consultez les écrans suivantes pour superviser le trafic de la grappe :

- **show conn [detail], cluster exec show conn**

  La commande **show conn** indique si un flux est un flux de directeur, de sauvegarde ou de transfert. Utilisez la commande **cluster exec show conn** sur n'importe quel nœud pour afficher toutes les connexions. Cette commande peut montrer comment le trafic d'un flux unique arrive à différents ASA dans la grappe. Le débit de la grappe dépend de l'efficacité et de la configuration de l'équilibrage de charges. Cette commande offre un moyen simple d'afficher le trafic d'une connexion dans la grappe et peut vous aider à comprendre comment un équilibreur de charges peut affecter les performances d'un flux.

  La commande **show conn detail** indique également quels flux sont soumis à la mobilité des flux.

  L'exemple suivant illustre une sortie de la commande **show conn detail** :

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
```

```
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic received
 at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface NP
Identity
Ifc Locally received: 716 (8 byte/s)
```

Pour dépanner le flux de connexion, observez d'abord les connexions sur tous les nœuds en saisissant la commande **cluster exec show conn** sur n'importe quel nœud. Recherchez les flux qui ont les indicateurs suivants : directeur (Y), sauvegarde (y) et transitaire (z). L'exemple suivant montre une connexion SSH de 172.18.124.187:22 à 192.168.103.131:44727 sur les trois ASA; l'ASA 1 a l'indicateur z indiquant qu'il s'agit d'un transitaire pour la connexion, l'ASA 3 a l'indicateur y indiquant qu'il est le directeur de la connexion et l'ASA 2 n'a pas d'indicateurs spéciaux indiquant qu'il est le propriétaire. Dans le sens sortant, les paquets de cette connexion pénètrent dans l'interface interne de l'ASA 2 et quittent l'interface externe. Dans le sens entrant, les paquets de cette connexion pénètrent dans l'interface externe sur l'ASA 1 et l'ASA 3, sont acheminés sur la liaison de commande de grappe vers l'ASA 2, puis quittent l'interface interne sur l'ASA 2.

```
ciscoasa/ASA1/control node# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**********************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO
```

```
ASA3:**************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  Les commandes **show cluster info conn-distribution** et **show cluster info packet-distribution** affichent la distribution du trafic sur tous les nœuds de la grappe. Ces commandes peuvent vous aider à évaluer et à ajuster l'équilibreur de charges externe.

  La commande **show cluster info loadbalance** affiche les statistiques de rééquilibrage des connexions.

  La commande **show cluster info flow-mobility counters** affiche les renseignements sur le mouvement de l'EID et le mouvement du propriétaire du flux. Consultez la sortie suivante pour **show cluster info flow-mobility counters** :

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  La commande **show cluster info load-monitor** affiche la charge de trafic pour les membres de la grappe pour le dernier intervalle ainsi que la moyenne du nombre total d'intervalles configurés (30 par défaut). Utilisez le mot clé **details** pour afficher la valeur de chaque mesure à chaque intervalle.

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 30 interval:
   0           0            0            12              28
   1           0            0            13              27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval



Connection count captured over 30 intervals:

Unit ID  0
```

```
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
Unit ID  1
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0

Buffer drops captured over 30 intervals:
Unit ID  0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
Unit ID  1
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
       25         25         30         30         30         35
       25         25         35         30         30         30
       25         25         30         25         25         35
       30         30         30         25         25         25
```

```
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35


CPU usage(%) captured over 30 intervals:
Unit ID  0
        25          25          30          30          30          35
        25          25          35          30          30          30
        25          25          30          25          25          35
        30          30          30          25          25          25
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  Affiche les données agrégées pour l'ensemble de la grappe. Les *options* disponibles dépendent du type de données.

  Consultez la sortie suivante pour la commande **show cluster access-list** :

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
```

```
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

Pour afficher le nombre agrégé des connexions utilisées pour tous les nœuds, saisissez :

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):**************************************************************
  100 in use, 100 most used

  cl1:*********************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  Cette commande est utile pour le dépannage des chemins de données.

Supervision du routage de la grappe

Consultez les commandes suivantes pour le routage de la grappe :

- **show route cluster**
- **debug route cluster**

  Affiche les renseignements sur la grappe pour le routage.

- **show lisp eid**

  Affiche le tableau EID de l'ASA qui indique les EID et les ID de site.

  Consultez la sortie suivante de la commande **cluster exec show lisp eid**.

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):**********************************************************
```

```
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:*****************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  Cette commande est utile pour la résolution de problèmes.

Configuration de la journalisation pour la mise en grappe

Consultez la commande suivante pour configurer la journalisation pour la mise en grappe :

logging device-id

Chaque nœud de la grappe génère des messages de journal système de manière indépendante. Vous pouvez utiliser la commande **logging device-id** pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant de nœuds identiques ou différents dans la grappe.

Supervision des interfaces de grappe

Consultez les commandes suivantes pour superviser les interfaces de la grappe :

- **show cluster interface-mode**

  Affiche le mode d'interface de la grappe.

Débogage de la mise en grappe

Consultez les commandes suivantes pour le débogage de la mise en grappe :

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  Affiche les messages de débogage pour la mise en grappe.

- **debug cluster flow-mobility**

  Affiche les événements liés à la mobilité des flux de mise en grappe.

- **debug lisp eid-notify-intercept**

  Affiche les événements lorsque le message eid-notify est intercepté.

- **show cluster info trace**

  La commande **show cluster info trace** affiche les renseignements de débogage pour un dépannage ultérieur.

  Consultez la sortie suivante pour la commande **show cluster info trace** :

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

Par exemple, si vous voyez les messages suivants indiquant que deux nœuds ayant le même nom **local-unit** agissent en tant que nœud de contrôle, cela peut signifier que deux nœuds ont le même nom **local-unit** (vérifiez votre configuration) ou qu'un nœud reçoit ses propres messages de diffusion (vérifiez votre réseau).

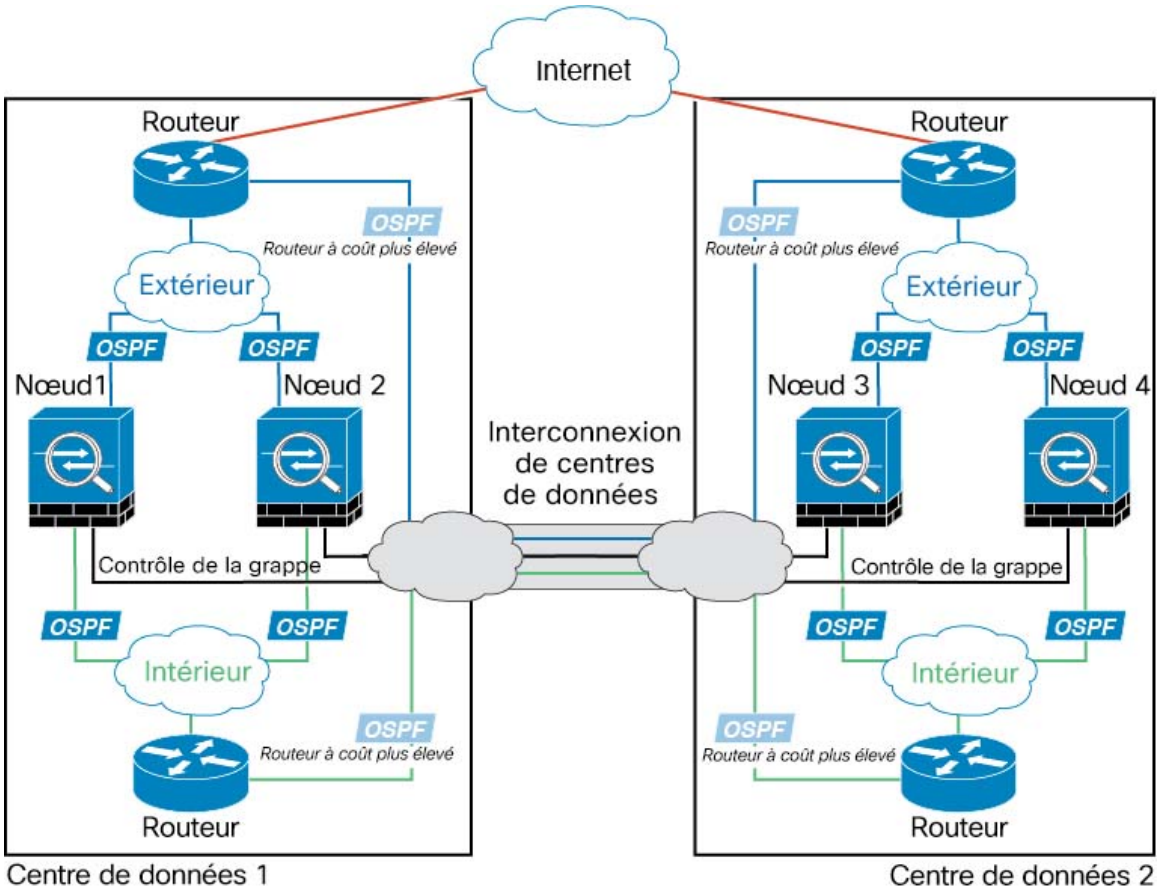
```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node
 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

Exemples de mise en grappe d'ASA virtuel

Ces exemples incluent toutes les configurations ASA liées aux grappes pour les déploiements typiques.

Exemple inter-sites nord-sud de mode routé d'interface individuelle

L'exemple suivant montre 2 nœuds de grappe ASA dans chacun des 2 centres de données placés entre les routeurs internes et externes (insertion nord-sud). Les nœuds de la grappe sont connectés par la liaison de commande de grappe sur l'interface DCI. Les routeurs internes et externes de chaque centre de données utilisent OSPF et PBR ou ECMP pour équilibrer la charge du trafic entre les membres de la grappe. En attribuant un routage à coût plus élevé sur l'interface DCI, le trafic reste dans chaque centre de données, sauf si tous les nœuds de la grappe ASA d'un site donné tombent en panne. En cas de défaillance de tous les nœuds de la grappe sur un site, le trafic passe de chaque routeur sur l'interface DCI aux nœuds de la grappe ASA sur l'autre site.



Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe de l'ASA

Certaines fonctionnalités d'ASA ne sont pas prises en charge avec la mise en grappe d'ASA, et d'autres le sont uniquement sur le nœud de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

- Fonctionnalités de communication unifiée qui reposent sur le mandataire TLS
- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Interfaces de tunnel virtuel (VTI)
- Les inspections d'application suivantes :

- CTIQBE
- H323, H225 et RAS
- Intercommunication IPsec
- MGCP
- MMP
- RTSP
- SCCP (Skinny)
- WAAS
- WCCP

- Filtre de trafic de réseau de zombies
- Auto Update Server
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Équilibrage de la charge VPN
- Basculement
- Routage et pont intégrés
- Mode FIPS

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.



Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS

- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SunRPC
- TFTP
- XDMCP

- Surveillance du routage statique
- Autorisation et authentification pour l'accès réseau La comptabilité est décentralisée.
- Services de filtrage
- VPN de site à site
- Routage multidiffusion

Fonctionnalités appliquées aux nœuds individuels

Ces fonctionnalités sont appliquées à chaque nœud ASA, plutôt qu'à la grappe dans son ensemble ou au nœud de contrôle.

- QoS : la politique QoS est synchronisée dans la grappe dans le cadre de la duplication de la configuration. Cependant, la politique est appliquée sur chaque nœud indépendamment. Par exemple, si vous configurez le contrôle en sortie, les valeurs de débit de conformité et de rafale de conformité s'appliquent au trafic sortant d'un ASA particulier. Dans une grappe à 3 nœuds et avec le trafic réparti uniformément, le taux de conformité devient en fait trois fois supérieur au débit de la grappe.
- Détection des menaces : la détection des menaces fonctionne sur chaque nœud indépendamment; par exemple, les statistiques principales sont propres au nœud. La détection de l'analyse de port, par exemple, ne fonctionne pas, car l'analyse du trafic sera équilibrée entre tous les nœuds et un nœud ne verra pas tout le trafic.
- Gestion des ressources : la gestion des ressources en mode contexte multiple est appliquée séparément sur chaque nœud en fonction de l'utilisation locale.
- Trafic LISP : le trafic LISP sur le port UDP 4342 est inspecté par chaque nœud de réception, mais aucun directeur n'est affecté. Chaque nœud ajoute au tableau EID qui est partagé dans la grappe, mais le trafic LISP lui-même ne participe pas au partage de l'état de la grappe.

AAA pour l'accès réseau et la mise en grappe

L'AAA pour l'accès réseau comprend trois composants : l'authentification, l'autorisation et la gestion de comptes. L'authentification et l'autorisation sont mises en œuvre en tant que fonctionnalités centralisées sur le nœud de contrôle de mise en grappe avec la duplication des structures de données sur les nœuds de données de grappe. Si un nœud de contrôle est choisi, le nouveau nœud de contrôle disposera de toute l'information nécessaire pour continuer le fonctionnement ininterrompu des utilisateurs authentifiés établis et de leurs

autorisations associées. Les délais d'inactivité et absolue pour l'authentification des utilisateurs sont conservés lors d'un changement de nœud de contrôle se produit.

La comptabilité est mise en œuvre en tant que fonctionnalité distribuée dans une grappe. La comptabilité est effectuée flux par flux, de sorte que le nœud de la grappe possédant un flux enverra les messages de démarrage et d'arrêt de comptabilité au serveur AAA lorsque la comptabilité est configurée pour un flux.

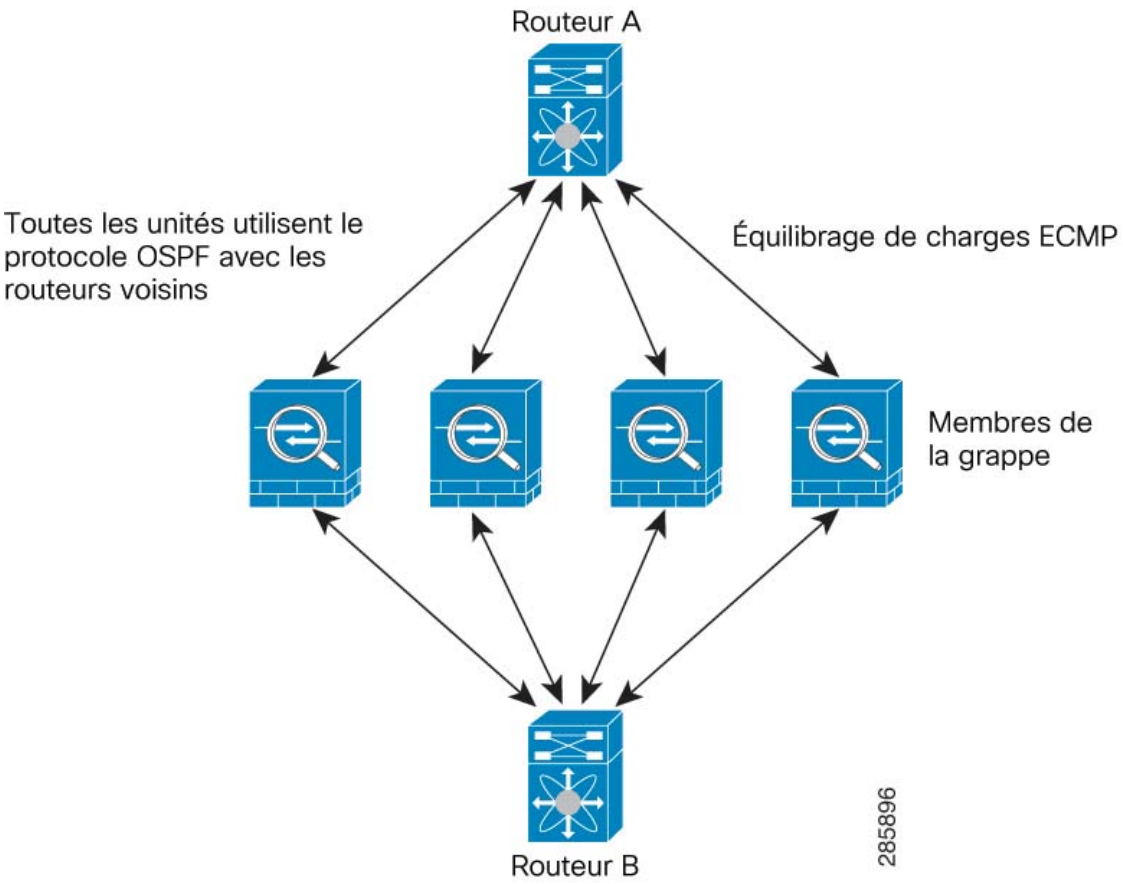
Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe (voir les commandes **set connection conn-max**, **set connection embryonic-conn-max**, **set connection per-client-embryonic-max**, et **set connection per-client-max**). Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

Routage et mise en grappe dynamiques

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 54 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Remarque Si la grappe comporte plusieurs contiguïtés avec le même routeur à des fins de redondance, le routage dissymétrique peut entraîner une perte de trafic inacceptable. Pour éviter le routage dissymétrique, regroupez toutes ces interfaces de nœud dans la même zone de trafic. Voir Configurer une zone de trafic, à la page 822.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.
- Si vous utilisez l'AAA pour l'accès FTP, le flux du canal de contrôle est centralisé sur le nœud de contrôle.

Inspection ICMP et mise en grappe

Le flux des paquets d'erreurs ICMP et ICMP dans la grappe varie selon que l'inspection d'erreurs ICMP ou ICMP est activée ou non. Sans inspection ICMP, ICMP est un flux unidirectionnel et il n'y a pas de prise en charge de flux directeur. Avec l'inspection ICMP, le flux ICMP devient bidirectionnel et est soutenu par un flux directeur/de sauvegarde. L'une des différences avec un flux ICMP inspecté réside dans le traitement par le directeur du paquet transféré : le directeur transmettra le paquet de réponse d'écho ICMP au propriétaire du flux au lieu de retourner le paquet au transitaire.

Routage multidiffusion et mise en grappe

En mode d'interface individuel, les unités n'agissent pas indépendamment avec la multidiffusion. Toutes les données et les paquets de routage sont traités et transmis par l'unité de contrôle, évitant ainsi la duplication des paquets.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents ASAdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à ASA qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- No Proxy ARP (Pas de serveur mandataire ARP) : pour les interfaces individuelles, une réponse de serveur mandataire ARP n'est jamais envoyée pour les adresses mappées. Cela empêche le routeur adjacent de maintenir une relation d'homologue avec un ASA qui ne fait plus partie de la grappe. Le routeur en amont a besoin d'une route statique ou d'un PBR avec suivi d'objets pour les adresses mappées qui pointe vers l'adresse IP de la grappe principale. Ce n'est pas un problème pour un EtherChannel étendu, car il n'y a qu'une seule adresse IP associée à l'interface de grappe.
- No interface PAT on an Individual interface (Pas de PAT d'interface sur une interface individuelle) Le PAT d'interface n'est pas pris en charge pour les interfaces individuelles.
- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.
- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, la grappe divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.
- Réutiliser un pool PAT dans plusieurs règles : pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.

- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.
- Fonctionnalité PAT par session : bien qu'elle ne soit pas exclusive à la mise en grappe, la fonctionnalité PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque nœud de données de posséder des connexions PAT; en revanche, les connexions PAT multisessions doivent être transférées au nœud de contrôle et détenues par celui-ci. Par défaut, tout le trafic TCP et le trafic DNS UDP utilisent un xlate PAT par session, tandis que ICMP et tout le reste du trafic UDP utilise la multisession. Vous pouvez configurer des règles NAT par session pour modifier ces valeurs par défaut pour TCP et UDP, mais vous ne pouvez pas configurer la PAT par session pour ICMP. Par exemple, en raison de l'utilisation croissante du protocole Quic sur le port UDP/443 comme alternative de performance à HTTPS TLS sur TCP/443, vous devriez activer la traduction d'adresses par session (PAT) pour UDP/443. Pour le trafic qui bénéficie de la PAT multisession, comme le H.323, le SIP ou l'interface simplifiée, vous pouvez désactiver la PAT par session pour les ports TCP associés (les ports UDP de ces ports H.323 et SIP sont déjà multisession en par défaut). Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.
- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

SCTP et mise en grappe

Une association SCTP peut être créée sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses connexions multi-hébergement doivent résider sur le même nœud.

Inspection SIP et mise en grappe

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

La configuration du mandataire TLS n'est pas prise en charge.

SNMP et mise en grappe

Un agent SNMP interroge chaque ASA en fonction de l'adresse IP locale de son . Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud.Vous devez les rajouter sur le nœud de contrôle pour forcer les utilisateurs à se reproduire vers le nouveau nœud, ou directement sur le nœud de données.

STUN et mise en grappe

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Syslog, NetFlow et la mise en grappe

- Syslog : chaque nœud de la grappe génère ses propres messages de journal système. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.
- NetFlow : chaque nœud de la grappe génère son propre flux NetFlow. Le collecteur NetFlow peut traiter chaque appareil ASA uniquement comme un exportateur NetFlow distinct.

Cisco TrustSec et la mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; seul le nœud de contrôle prend en charge les connexions VPN.



Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Pour les connexions à une interface individuelle lors de l'utilisation de PBR ou d'ECMP, vous devez toujours vous connecter à l'adresse IP de la grappe principale, et non à une adresse locale.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

Choix du nœud de contrôle

Les nœuds de la grappe communiquent sur la liaison de commande de grappe pour élire un nœud de contrôle comme suit :

1. Lorsque vous activez la mise en grappe pour un nœud (ou lorsqu'il démarre avec la mise en grappe déjà activée), il diffuse une demande de sélection toutes les 3 secondes.
2. Tous les autres nœuds ayant une priorité plus élevée répondent à la demande de sélection; la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.

Remarque Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud se joint ultérieurement à la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle; le nœud de contrôle existant demeure toujours le nœud de contrôle, sauf s'il s'arrête de répondre, moment auquel un nouveau nœud de contrôle est sélectionné.
5. Dans un scénario de « discernement partagé », où il y a temporairement plusieurs nœuds de contrôle, le nœud ayant la priorité la plus élevée conserve le rôle tandis que les autres nœuds retournent aux rôles de nœud de données.

Remarque Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Haute disponibilité au sein de la grappe ASA virtuel

La mise en grappe ASA virtuel assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

Surveillance de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Consultez Choix du nœud de contrôle, à la page 606 pour de plus amples renseignements.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

Lorsque vous activez la surveillance de l'intégrité, toutes les interfaces physiques sont supervisées par défaut; vous pouvez éventuellement désactiver la surveillance par interface. Seules les interfaces nommées peuvent être surveillées.

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le délai avant la suppression par l'ASA d'un membre de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. L'ASA ne supervise pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de l'ASA de la grappe. Le nœud est supprimé après 500 ms, quel que soit son état.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

ASA tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque ASA devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Rejoindre la grappe

Après le retrait d'un nœud de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe au niveau de l'interface de ligne de commande en saisissant la commande **cluster group** *name*, puis **enable**.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : l'ASA essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment. Ce comportement est configurable.
- Échec de l'interface de données : l'ASA tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'ASA désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe au niveau de l'interface de ligne de commande en saisissant la commande **cluster group** *name*, puis **enable**. Ce comportement est configurable.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que la liaison de commande de grappe soit active et que la mise en grappe soit toujours activée avec la commande **enable**. L'ASA tente de rejoindre la grappe toutes les 5 secondes.
- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc. Un nœud tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Ce comportement est configurable.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 20 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
Tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	Comprend les règles AAA (uauth).
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—
VPN distribué (site à site) pour Firepower 4100/9300	Oui	La session de sauvegarde devient la session active, puis une nouvelle session de sauvegarde est créée.

Gestion des connexions par la grappe ASA virtuel

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- Propriétaire du sauvegarde : nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis.

Si vous activez la localisation du directeur pour la mise en grappe inter-sites, il existe deux rôles de propriétaire de la sauvegarde : le rôle de sauvegarde locale et de sauvegarde globale. Le propriétaire choisit toujours une sauvegarde locale sur le même site que lui (en fonction de l'ID du site). La sauvegarde globale peut se trouver sur n'importe quel site et peut même se trouver sur le même nœud que la sauvegarde locale. Le propriétaire envoie des informations sur l'état de la connexion aux deux sauvegardes.

Si vous activez la redondance de sites et que le propriétaire de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La sauvegarde de châssis et la sauvegarde de site sont indépendantes. Par conséquent, dans certains cas, un flux comportera à la fois une sauvegarde de châssis et une sauvegarde de site.

- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Si vous activez la localisation de directeur pour la mise en grappe inter-sites, il y a deux rôles de directeur : le directeur local et le directeur global. Le propriétaire choisit toujours un directeur local sur le même site que lui (en fonction de l'ID du site). Le directeur global peut être sur n'importe quel site et peut même être le même nœud que le directeur local. En cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site.

  Détails du hachage ICMP/ICMPv6 :

  - Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
  - Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
  - Pour les autres paquets, les ports source et de destination sont à 0.

- Transitaire : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Si vous activez la localisation de directeur, le redirecteur interroge toujours le directeur local. Le transitaire n'interroge le directeur global que si le directeur local ne connaît pas le propriétaire, par exemple, si un membre de la grappe reçoit des paquets pour une connexion qui appartient à un autre site. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.

Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- Propriétaire de fragment : pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Connexions par traduction d'adresse de port

Lorsqu'une connexion utilise la traduction d'adresses de port (PAT), le type de PAT (par session ou multisession) influence quel membre de la grappe devient propriétaire de la nouvelle connexion :

- PAT par session : le propriétaire est le nœud qui reçoit le paquet initial dans la connexion.

  Par défaut, le trafic TCP et DNS UDP utilise une PAT par session.

- PAT multisession : le propriétaire est toujours le nœud de contrôle. Si une connexion PAT multisession est initialement reçue par un nœud de données, le nœud de données transfère la connexion au nœud de contrôle.

  Par défaut, le trafic UDP (à l'exception du trafic UDP DNS) et ICMP utilise la PAT multisession. Ces connexions appartiennent donc toujours au nœud de contrôle.

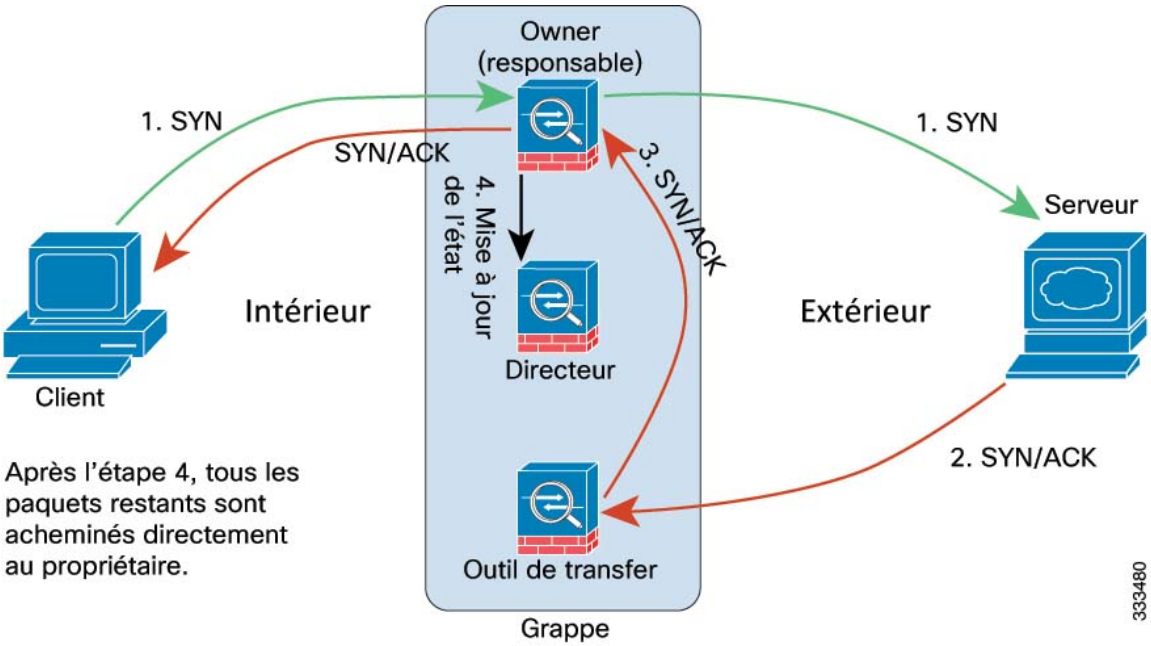
Vous pouvez modifier les valeurs par défaut de PAT par session pour les protocoles TCP et UDP afin que les connexions à ces protocoles soient gérées par session ou multisession selon la configuration. Pour ICMP, vous ne pouvez pas modifier la PAT multisession par défaut. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Pour de meilleures performances, un bon équilibrage de la charge externe est nécessaire pour que les deux directions d'un flux arrivent au même nœud et pour que les flux soient répartis uniformément entre les nœuds. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

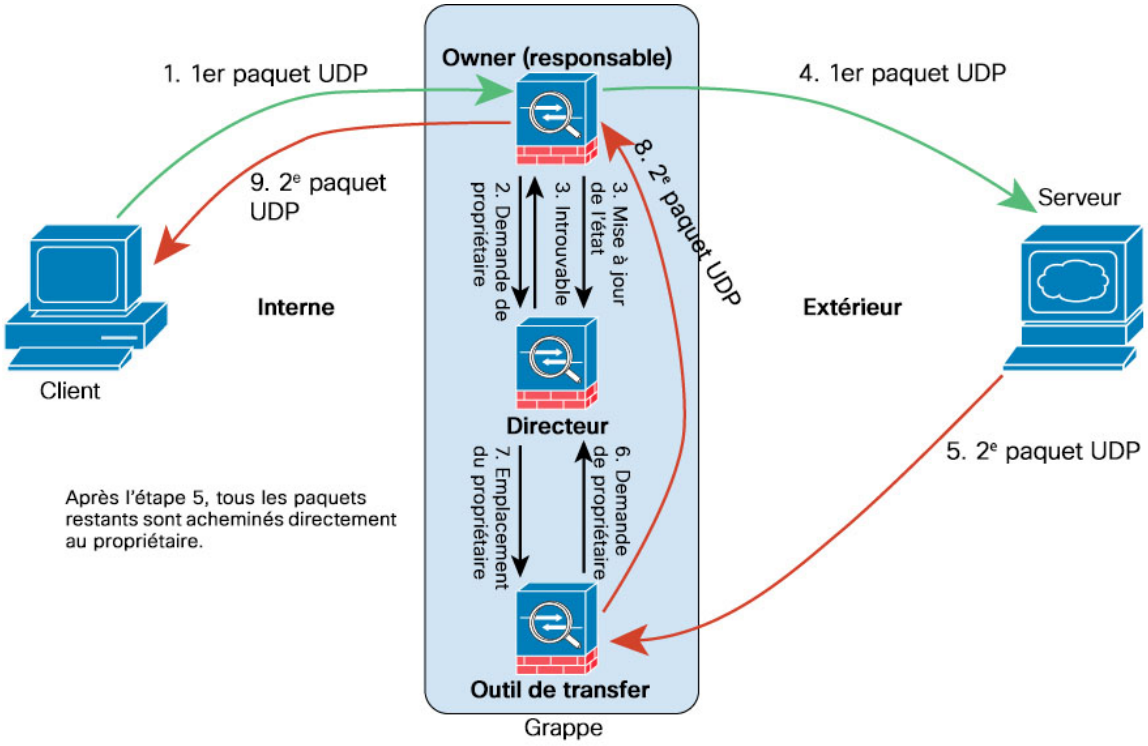


1. Le paquet SYN provient du client et est livré à un ASA (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un ASA différent (selon la méthode d'équilibrage de la charge). Cet ASA est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.
5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. ***Illustration 55 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un ASA (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.
6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Rééquilibrage des nouvelles connexions TCP dans la grappe

Si les capacités d'équilibrage de charges des routeurs en amont ou en aval entraînent une répartition non équilibrée des flux, vous pouvez configurer un rééquilibrage des nouvelles connexions afin que les nœuds

ayant le plus de nouvelles connexions par seconde redirigent les nouveaux flux TCP vers d'autres nœuds. Aucun flux existant ne sera déplacé vers d'autres nœuds.

Comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Historique de la mise en grappe d'ASA virtuel

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Suppression des propos tendancieux	9.19(1)	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
Mise en grappe d'ASAv30, ASAv50 et ASAv100 pour VMware et KVM	9.17(1)	La mise en grappe d'ASA virtuel vous permet de regrouper jusqu'à 16 ASA virtuel en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. La mise en grappe d'ASA virtuel prend en charge le mode d'interface individuelle en mode de pare-feu routé; les EtherChannels étendus ne sont pas pris en charge. L'ASA virtuel utilise une interface virtuelle VNI (VXLAN) pour la liaison de commande de grappe. Commandes nouvelles ou modifiées : **cluster-interface vni**, **nve-only cluster**, **peer-group**, **show cluster info**, **show cluster info instance-type**, **show nve 1**



CHAPITRE 13

Grappe ASA pour l'ASA virtuel dans un nuage public

La mise en grappe vous permet de regrouper plusieurs ASA virtuel en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. Vous pouvez déployer des grappes ASA virtuel dans un nuage public en utilisant les éléments suivants :

- Amazon Web Services (AWS)

Actuellement, seul le mode pare-feu routé est pris en charge.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 653.

- À propos de la mise en grappe d'ASA virtuel dans le nuage public, à la page 615
- Licences pour la mise en grappe d'ASA virtuel, à la page 620
- Exigences et conditions préalables à la mise en grappe d'ASA virtuel, à la page 620
- Lignes directrices relatives à la mise en grappe d'ASA virtuel, à la page 622
- Déployer la grappe dans AWS, à la page 623
- Personnaliser l'opération de mise en grappe, à la page 633
- Gérer les nœuds de la grappe, à la page 637
- Surveillance de la grappe, à la page 641
- Référence pour la mise en grappe, à la page 652
- Historique de la mise en grappe d'ASA virtuel dans le nuage public, à la page 668

À propos de la mise en grappe d'ASA virtuel dans le nuage public

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

Intégration de la grappe dans votre réseau

La grappe se compose de plusieurs pare-feu agissant comme un seul périphérique. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau isolé pour la communication intra-grappe, appelé *liaison de commande de grappe*, qui utilise des interfaces VXLAN. Les VXLAN, qui agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3, permettent à la ASA virtuel d'envoyer des messages en diffusion ou en multidiffusion sur la liaison de commande de grappe.
- Équilibreur(s) de charges : pour l'équilibrage de charges externe, vous avez les options suivantes :
  - Équilibreur de charge de passerelle AWS

    L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. Le ASA virtuel prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point terminal de l'équilibreur de charge de passerelle) à l'aide d'un serveur mandataire à un seul bras d'interface de Geneve.
  - Routage à chemins multiples à coût égal (ECMP) utilisant des routeurs internes et externes comme le routeur des services en nuage de Cisco

    Le routage ECMP peut transférer des paquets sur plusieurs « meilleurs chemins » qui se partagent la première place dans la mesure du routage. Comme pour l'EtherChannel, un hachage des adresses IP source et de destination ou des ports source et de destination peut être utilisé pour envoyer un paquet vers l'un des sauts suivants. Si vous utilisez des routes statiques pour le routage ECMP, la défaillance de ASA virtuel peut provoquer des problèmes. le routage continue d'être utilisé et le trafic vers le ASA virtuel défaillant sera perdu. Si vous utilisez des routes statiques, veillez à utiliser une fonctionnalité de surveillance de routage statique telle que le suivi d'objets. Nous recommandons d'utiliser des protocoles de routage dynamique pour ajouter et supprimer des routes, auquel cas vous devez configurer chaque ASA virtuel pour qu'il participe au routage dynamique.



Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge pour l'équilibrage de la charge.

Nœuds de la grappe

Les membres du nœud collaborent pour partager la politique de sécurité et les flux de trafic. Cette section décrit la nature du rôle de chaque nœud.

Configuration du démarrage

Sur chaque appareil, vous configurez une configuration de démarrage minimale qui inclut le nom de la grappe, l'interface de la liaison de commande de grappe et les autres paramètres de la grappe. Le premier nœud sur lequel vous activez la mise en grappe devient généralement le nœud de *contrôle*. Lorsque vous activez la mise en grappe sur les nœuds suivants, ils rejoignent la grappe en tant que nœuds de *données*.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité dans la configuration de démarrage. la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds de données. En règle générale, lorsque vous créez une grappe pour la première fois, le premier nœud que vous ajoutez devient le nœud de contrôle simplement parce que c'est le seul nœud de la grappe à ce moment-là.

Vous devez effectuer toute la configuration (à l'exception de la configuration de démarrage) sur le nœud de contrôle uniquement; la configuration est ensuite reproduite sur les nœuds de données. Dans le cas de ressources physiques, telles que les interfaces, la configuration du nœud de contrôle est reflétée sur tous les nœuds de données. Par exemple, si vous configurez Ethernet 1/2 comme interface interne et Ethernet 1/1 comme interface externe, ces interfaces sont également utilisées sur les nœuds de données en tant qu'interfaces interne et externe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

Interfaces individuelles

Vous pouvez configurer les interfaces de grappe en tant *qu'interfaces individuelles*.

Les interfaces individuelles sont des interfaces de routage normales, chacune avec sa propre adresse IP locale. La configuration d'interface doit être configurée uniquement sur le nœud de contrôle et chaque interface utilise DHCP.

Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Liaison de commande de grappe

Chaque nœud doit dédier une interface en tant qu'interface VXLAN (VTEP) pour la liaison de commande de grappe. Pour en savoir plus sur VXLAN, consultez Interfaces VXLAN, à la page 735.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP comporte deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier), et une interface normale appelée interface source du VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

Interface de la source VTEP

L'interface source du VTEP est une interface ASA virtuel classique à laquelle vous prévoyez associer l'interface VNI. Vous pouvez configurer une interface source de VTEP pour qu'elle agisse en tant que liaison de commande de grappe. L'interface source est réservée à une utilisation avec la liaison de commande de grappe uniquement. Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Interface VNI

Une interface VNI est semblable à une interface VLAN : il s'agit d'une interface virtuelle qui sépare le trafic réseau sur une interface physique donnée au moyen de balisage. Vous ne pouvez configurer qu'une seule interface VNI. Chaque interface VNI possède une adresse IP sur le même sous-réseau.

VTEP homologues

Contrairement au VXLAN habituel pour les interfaces de données, qui autorise un seul homologue VTEP, la mise en grappe ASA virtuel vous permet de configurer plusieurs homologues.

Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Échec de la liaison de commande de grappe

Si le protocole de liaison de commande de grappe tombe en panne pour une unité, la mise en grappe est désactivée; les interfaces de données sont fermées. Après avoir corrigé la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.



Remarque Lorsque l'ASA virtuel devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que l'unité a reçue du DHCP ou de l'ensemble d'adresses IP de la grappe. Si vous utilisez un ensemble d'adresses IP de grappe, si vous rechargez et que l'unité est toujours inactive dans la grappe, l'interface de gestion n'est pas accessible (car elle utilise alors l'adresse IP principale, qui est la même que le nœud de contrôle). Vous devez utiliser le port de console (si disponible) pour toute autre configuration.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

Gestion des grappes ASA virtuel

L'un des avantages de l'utilisation de la mise en grappe ASA virtuel est la facilité de gestion. Cette section décrit comment gérer la grappe.

Réseau de gestion

Nous vous conseillons de connecter tous les nœuds à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Interface de gestion

Utilisez l'interface Management 0/0 pour la gestion.

Remarque Vous ne pouvez pas activer le routage dynamique pour l'interface de gestion. Vous devez utiliser une route statique.

Vous pouvez utiliser l'adressage statique ou DHCP pour l'adresse IP de gestion.

Si vous utilisez l'adressage statique, vous pouvez utiliser l'adresse IP de la grappe principale qui est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle actuel. Pour chaque interface, vous configurez également une plage d'adresses de sorte que chaque nœud, y compris le nœud de contrôle actuel, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de gestion cohérent à une adresse; lorsqu'un nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente. L'adresse IP locale est utilisée pour le routage et est également utile pour la résolution de problèmes. Par exemple, vous pouvez gérer la grappe en vous connectant à l'adresse IP de la grappe principale, qui est toujours associée au nœud de contrôle actuel. Pour gérer un membre, vous pouvez vous connecter à l'adresse IP locale. Pour le trafic de gestion sortant tel que TFTP ou le journal système, chaque nœud, y compris le nœud de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Si vous utilisez DHCP, vous n'utilisez pas un ensemble d'adresses locales ou n'avez pas d'adresse IP de grappe principale.

Remarque Le trafic vers la boîte doit être acheminé vers l'adresse IP de gestion du nœud; le trafic vers la boîte n'est pas transféré sur la liaison de commande de grappe vers un autre nœud.

Gestion de nœud de contrôle vs Gestion de nœud de données

Toutes la gestion et la surveillance peuvent avoir lieu sur le nœud de contrôle. À partir du nœud de contrôle, vous pouvez vérifier les statistiques d'exécution, l'utilisation des ressources ou d'autres informations de surveillance sur tous les nœuds. Vous pouvez également transmettre une commande à tous les nœuds de la grappe et reproduire les messages de console des nœuds de données vers le nœud de contrôle.

Vous pouvez surveiller directement les nœuds de données si vous le souhaitez. Bien que cela soit également disponible à partir du nœud de contrôle, vous pouvez effectuer la gestion de fichiers sur les nœuds de données (y compris la sauvegarde de la configuration et la mise à jour des images). Les fonctions suivantes ne sont pas disponibles à partir du nœud de commande :

- Surveillance des statistiques propres à la grappe par nœud.
- Surveillance des journaux système par nœud (sauf pour les journaux système envoyés à la console lorsque la duplication de la console est activée).
- SNMP
- NetFlow

duplication de clé de chiffrement

Lorsque vous créez une clé de chiffrement sur le nœud de contrôle, la clé est répliquée sur tous les nœuds de données. Si vous avez une session SSH sur l'adresse IP de la grappe principale, vous serez déconnecté en cas de défaillance du nœud de contrôle. Le nouveau nœud de contrôle utilise la même clé pour les connexions SSH, de sorte que vous n'avez pas besoin de mettre à jour la clé d'hôte SSH mise en cache lorsque vous vous reconnectez au nouveau nœud de contrôle.

Incompatibilité d'adresse IP du certificat de connexion ASDM

Par défaut, un certificat autosigné est utilisé pour la connexion ASDM en fonction de l'adresse IP locale. Si vous vous connectez à l'adresse IP de la grappe principale à l'aide d'ASDM, un message d'avertissement concernant une adresse IP non concordante peut s'afficher, car le certificat utilise l'adresse IP locale, et non l'adresse IP de la grappe principale. Vous pouvez ignorer le message et établir la connexion ASDM. Cependant, pour éviter ce type d'avertissement, vous pouvez inscrire un certificat qui contient l'adresse IP de la grappe principale et toutes les adresses IP locales de l'ensemble d'adresses IP. Vous pouvez ensuite utiliser ce certificat pour chaque membre de la grappe. Consultez https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html pour de plus amples renseignements.

Licences pour la mise en grappe d'ASA virtuel

Chaque nœud de grappe nécessite la même licence de modèle. Nous vous conseillons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au membre le moins performant. Le niveau de débit sera répliqué du nœud de contrôle à chaque nœud de données afin qu'ils correspondent.

Remarque Si vous annulez l'enregistrement de l'ASA virtuel pour qu'il ne soit pas sous licence, il reviendra à un état de débit fortement limité si vous rechargez l'ASA virtuel. Un nœud de grappe sans licence et à faible performance aura une incidence négative sur les performances de l'ensemble de la grappe. Assurez-vous de conserver tous les nœuds de la grappe sous licence ou de supprimer les nœuds sans licence.

Exigences et conditions préalables à la mise en grappe d'ASA virtuel

Exigences du modèle

- ASAv30, ASAv50, ASAv100

- Les service de nuage public suivants :
  - Amazon Web Services (AWS)
- Maximum de 16 nœuds

Consultez également les exigences générales pour l'ASA virtuel dans le Guide de démarrage de l'ASA virtuel.

Configuration matérielle et logicielle requise

Tous les nœuds d'une grappe :

- Il doit s'agir du même niveau de performance. Nous vous conseillons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au nœud le moins performant.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Prise en charge du déploiement de zone de disponibilité unique.
- Les interfaces de liaison de commande de grappe doivent se trouver dans le même sous-réseau, de sorte que la grappe doit être déployée dans le même sous-réseau.

MTU

Assurez-vous que les ports connectés à la liaison de commande de grappe ont une MTU correcte (plus élevée) configurée. En cas de non-concordance MTU, la formation de la grappe échouera.

La MTU de la liaison de commande de grappe doit être 154 octets supérieure aux interfaces de données. Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets).

Pour AWS avec GWLB, l'interface de données utilise l'encapsulation de Geneve. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 306 octets. Ainsi, pour le chemin réseau standard de 1 500 MTU, la MTU de l'interface source doit être de 1 806 et la MTU de la liaison de commande de grappe doit être de +154, 1 960.

Le tableau suivant présente la MTU de la liaison de commande de grappe et la MTU de l'interface de données suggérées.

Remarque Nous ne recommandons pas de définir la MTU de la liaison de commande de grappe entre 2561 et 8362. En raison de la gestion du groupe de blocs, cette taille MTU n'est pas optimale pour le fonctionnement du système.

Tableau 21 : MTU suggérée

Nuage public	Liaison de commande de grappe	MTU de l'interface de données
AWS avec GWLB	1960	1806

Nuage public	Liaison de commande de grappe	MTU de l'interface de données
AWS	1654	1 500

Lignes directrices relatives à la mise en grappe d'ASA virtuel

Haute disponibilité

La haute disponibilité n'est pas prise en charge par la mise en grappe.

IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA virtuel ou le commutateur, ajout d'un commutateur supplémentaire pour former un système de commutation redondant), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.
- Lors de l'ajout d'un nœud à une grappe existante ou lors du rechargement d'un nœud, il se produit une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Pour les connexions TLS/SSL déchiffrées, les états de déchiffrement ne sont pas synchronisés, et si le propriétaire de la connexion échoue, les connexions déchiffrées sont réinitialisées. De nouvelles connexions devront être établies vers un nouveau nœud. Les connexions qui ne sont pas déchiffrées (elles correspondent à une règle « ne pas déchiffrer ») ne sont pas affectées et sont répliquées correctement.
- L'évolutivité dynamique n'est pas prise en charge.
- Le basculement avec état de la cible n'est pas pris en charge lorsque vous déployez la grappe sur AWS.
- Effectuer un déploiement global à la fin de chaque fenêtre de maintenance.
- Assurez-vous de ne pas supprimer plusieurs périphériques à la fois du groupe d'évolutivité automatique (AWS) ou de l'ensemble d'évolutivité (Azure). Nous vous conseillons également d'exécuter la commande **cluster disable** sur le périphérique avant de retirer ce périphérique du groupe d'évolutivité (AWS) ou de l'ensemble d'évolutivité (Azure).
- Si vous souhaitez désactiver les nœuds de données et le nœud de contrôle dans une grappe, nous vous recommandons de désactiver les nœuds de données avant de désactiver le nœud de contrôle. Si un nœud de contrôle est désactivé alors qu'il y a d'autres nœuds de données dans la grappe, l'un d'eux doit être promu au rang de nœud de contrôle. Notez que le changement de rôle pourrait perturber la grappe.

- Dans les scripts de configuration Day0 présentés dans ce guide, vous pouvez modifier les adresses IP selon vos besoins, fournir des noms d'interface personnalisés et modifier la séquence de l'interface CCL-Link.

Valeurs par défaut pour la mise en grappe

- L'ID du système cLACP est généré automatiquement et la priorité du système est 1 par défaut.
- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Déployer la grappe dans AWS

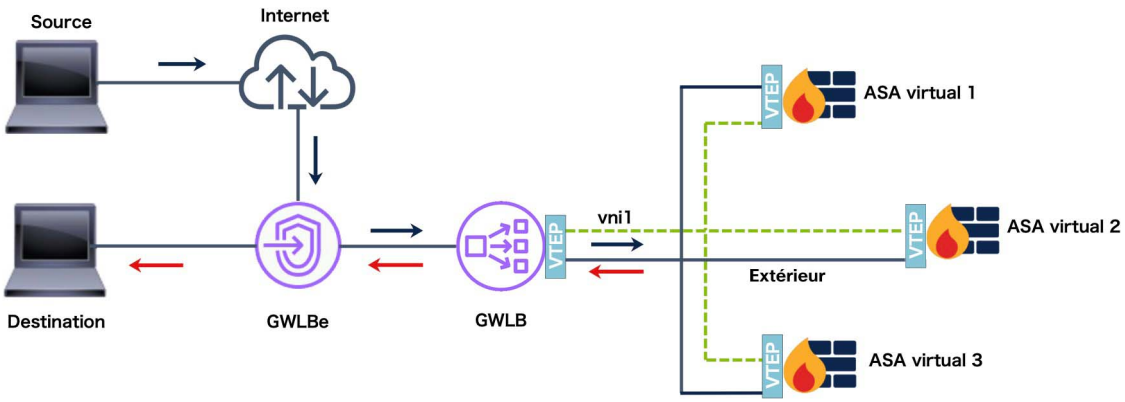
Pour déployer une grappe dans AWS, vous pouvez soit la déployer manuellement, soit utiliser des modèles CloudFormation pour déployer une pile. Vous pouvez utiliser la grappe avec l'équilibreur de charge de passerelle AWS ou avec un équilibreur de charge non natif comme le routeur des services en nuage de Cisco.

Équilibreur de charge de passerelle AWS et serveur mandataire à un seul volet de Geneve

Remarque Ce scénario est le seul actuellement pris en charge pour les interfaces de Geneve.

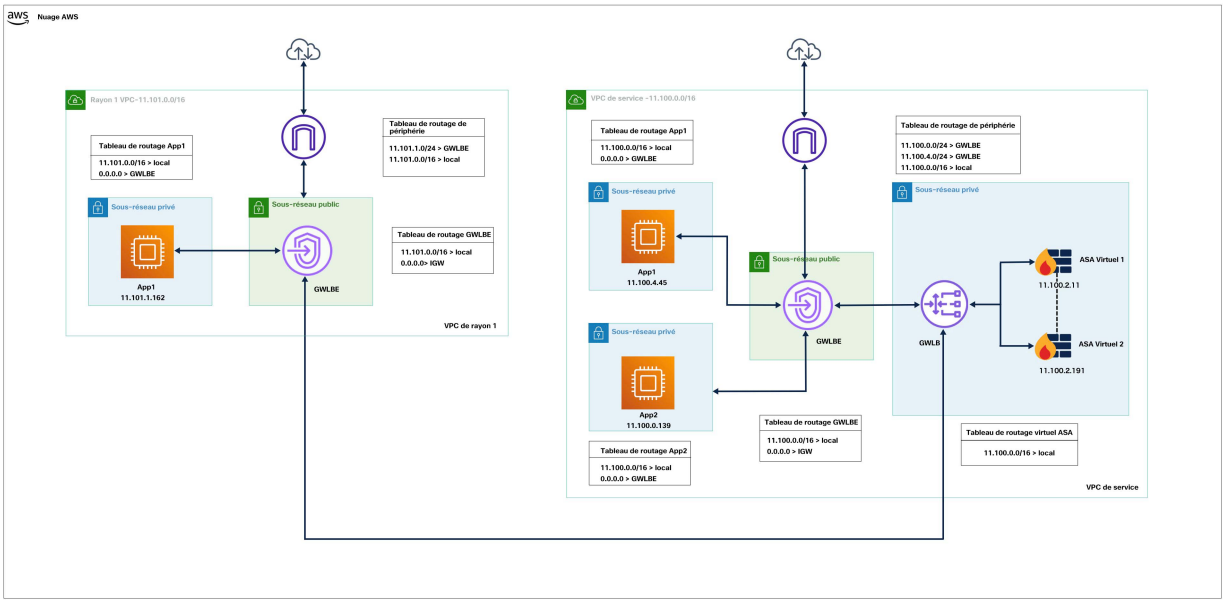
L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. L'ASA virtuel prend en charge le plan de commande centralisé de l'équilibreur de charges de passerelle avec un plan de données distribué (point terminal de l'équilibreur de charges de passerelle). La figure suivante montre le trafic acheminé vers l'équilibreur de charge de passerelle à partir du point terminal de l'équilibreur de charge de passerelle. L'équilibreur de charges de passerelle équilibre le trafic entre plusieurs ASA virtuels, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charges de passerelle (trafic à demi-tour). L'équilibreur de charge de passerelle renvoie ensuite le trafic au point terminal de l'équilibreur de charge de passerelle et à la destination.

Illustration 56 : Serveur mandataire à un seul volet Geneve



Exemple de topologie

La topologie indiquée ci-dessous décrit le flux de trafic entrant et sortant. Il y a deux instances ASA virtuel dans la grappe connectée à une GWLB.



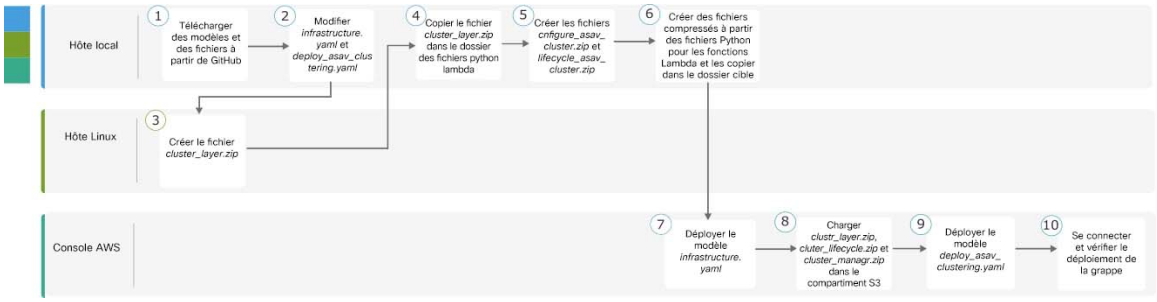
Le trafic entrant provenant d'Internet est dirigé vers le point terminal de la GWLB, qui le transmet ensuite à la GWLB. Le trafic est ensuite acheminé vers la grappe ASA virtuel. Une fois que le trafic a été inspecté par une instance ASA virtuel dans la grappe, il est transféré à la VM de l'application, App1.

Le trafic sortant d'App1 est transmis au point terminal de la GWLB, qui l'envoie ensuite vers Internet.

Processus de bout en bout pour le déploiement de la grappe ASA virtuel sur AWS

Déploiement basé sur un modèle

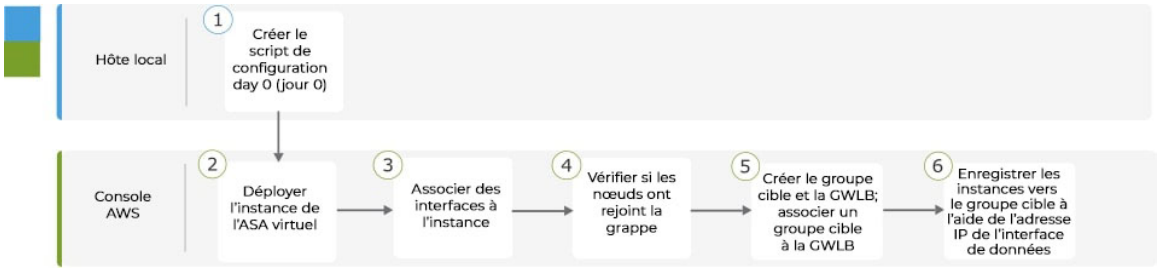
Le diagramme suivant illustre le flux de travail pour le déploiement basé sur le modèle de la grappe ASA virtuel sur AWS.



	Espace de travail	Étapes
1	Hôte local	Téléchargez des modèles et des fichiers à partir de GitHub.
2	Hôte local	Modifiez les modèles *infrastructure.yaml* et *deploying_asav_clustering.yaml*.
3	Hôte Linux	Créez le fichier *cluster_layer.zip*.
4	Hôte local	Copiez le fichier *cluster_layer.zip* dans le dossier des fichiers Python Lambda.
5	Hôte local	Créez les fichiers *configure_asav_cluster.zip* et *lifecycle_asav_cluster.zip*.
6	Hôte local	Créez des fichiers compressés à partir des fichiers Python pour les fonctions Lambda et les copier dans le dossier cible.
7	Console AWS	Déployez le modèle *infrastructure.yaml*.
8	Console AWS	Chargez cluster_layer.zip, cluster_lifecycle.zip et cluster_manager.zip dans le compartiment S3.
9	Console AWS	Déployez le modèle *deploy_asav_clustering.yaml*.
10	Console AWS	Connectez-vous et vérifiez le déploiement de la grappe.

Déploiement manuel

Le diagramme suivant illustre le flux de travail pour le déploiement manuel de la grappe ASA virtuel sur AWS.



	Espace de travail	Étapes
1	Hôte local	Créez le script de configuration de jour 0.
2	Console AWS	Déployez l'instance de l'ASA virtuel.
3	Console AWS	Associez des interfaces à l'instance.
4	Console AWS	Vérifiez si les nœuds ont rejoint la grappe.
5	Console AWS	Créez le groupe cible et la GWLB; associer un groupe cible à la GWLB.
6	Console AWS	Enregistrez les instances avec le groupe cible à l'aide de l'adresse IP de l'interface de données.

Modèles

Les modèles fournis ci-dessous sont disponibles dans GitHub. Les valeurs des paramètres sont explicites et les noms des paramètres, les valeurs par défaut, les valeurs autorisées et la description sont donnés dans le modèle.

- infrastructure.yaml : modèle pour le déploiement de l'infrastructure
- deploy_asav_clustering.yaml : modèle pour le déploiement en grappe.

Remarque Assurez-vous de consulter la liste des types d'instances AWS pris en charge avant de déployer les nœuds de la grappe. Cette liste se trouve dans le modèle *deploy_asav_clustering.yaml*, sous les valeurs autorisées pour le paramètre InstanceType (Type d'instance).

Déployer la pile dans AWS à l'aide d'un modèle CloudFormation

Déployez la pile dans AWS à l'aide du modèle personnalisé Cloud Formation.

Avant de commencer

- Vous avez besoin d'un ordinateur Linux avec Python 3.

Procédure

Étape 1 Préparez le modèle.

a) Copiez le référentiel github dans votre dossier local. Consultez https://github.com/CiscoDevNet/cisco-asav/tree/master/cluster/aws.

b) Modifiez **infrastructure.yaml** et **deploy_asav_clustering.yaml** avec les paramètres requis.

c) Créez un fichier nommé **cluster_layer.zip** pour fournir les bibliothèques Python essentielles aux fonctions Lambda.

Nous vous recommandons d'utiliser Amazon Linux avec Python 3.9 installé pour créer le fichier **cluster_layer.zip**.

Remarque
Si vous avez besoin d'un environnement Amazon Linux, vous pouvez créer une instance EC2 à l'aide de l'AMI d'Amazon Linux 2023 ou utiliser AWS Cloudshell, qui exécute la dernière version d'Amazon Linux.

Pour créer le fichier cluster-layer.zip, vous devez d'abord créer le fichier **requirements.txt** contenant les détails du paquet de la bibliothèque python, puis exécuter le script d'interface Shell.

1. Créez le fichier **requirements.txt** en précisant les détails du paquet Python.

   Voici un exemple de détails de paquet que vous fournissez dans le fichier **requirements.txt** :

   ```
   $ cat requirements.txt
   pycryptodome
   paramiko
   requests
   scp
   jsonschema
   cffi
   zipp
   importlib-metadata
   ```

2. Exécutez le script Shell suivant pour créer le fichier **cluster_layer.zip**.

   ```
   $ pip3 install --platform manylinux2014_x86_64
   --target=./python/lib/python3.9/site-packages
   --implementation cp --python-version 3.9 --only-binary=:all:
   --upgrade -r requirements.txt
   $ zip -r cluster_layer.zip ./python
   ```

Remarque
Si vous rencontrez une erreur de conflit de dépendances lors de l'installation, comme une erreur liée à urllib3 ou une erreur de cryptographie, il est recommandé d'inclure les paquets en conflit ainsi que leurs versions recommandées dans le fichier **requirements.txt**. Après cela, vous pouvez exécuter à nouveau l'installation pour résoudre le conflit.

d) Copiez le fichier **cluster_layer.zip** résultant dans le dossier des fichiers lambda python.

e) Créez les fichiers **configure_asav_cluster.zip** et **lifecycle_asav_cluster.zip**.

Un fichier make.py se trouve dans le répertoire supérieur du référentiel cloné. Cela compressera les fichiers python dans un fichier compressé et les copiera dans un dossier cible.

python3 make.py build

Étape 2 Déployez **infrastructure.yaml** et notez les valeurs de sortie pour le déploiement en grappe.

a) Sur la console AWS, accédez à **CloudFormation** et cliquez sur **Create stack** (Créer une pile); sélectionnez **With new resources (standard)** (Avec de nouvelles ressources (standard)).
b) Sélectionnez **Upload a template file** (Charger un fichier modèle), cliquez sur **Choose file** (Choisir un fichier) et sélectionnez **infrastructure.yaml** dans le dossier cible.
c) Cliquez sur **Next** (suivant) et fournissez les informations requises.
d) Cliquez sur **Next** (Suivant), puis sur **Create stack** (Créer une pile).
e) Une fois le déploiement terminé, accédez à **Outputs** (Résultats) et notez le nom de **compartiment** S3.

Illustration 57 : Sortie de infrastructure.yaml

Outputs (13)

Search outputs

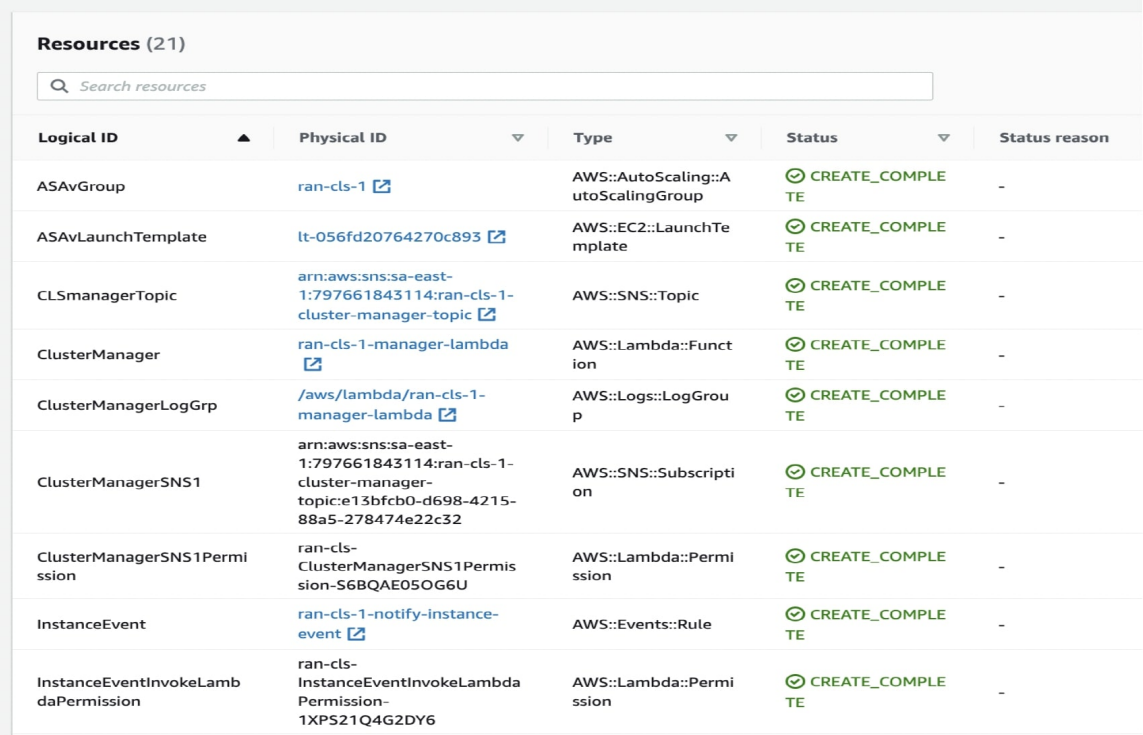
Key	Value	Description	Export name
AZ	sa-east-1a	Availability zone	-
BucketName	ran-cls-infra-s3bucketcluster-kckr7518u00l	Name of the Amazon S3 bucket	-
BucketUrl	http://ran-cls-infra-s3bucketcluster-kckr7518u00l.s3-website-sa-east-1.amazonaws.com	URL of S3 Bucket Static Website	-
CCLSubnetId	subnet-050feb347e57eba99	CCL subnet ID	-
EIPforNATgw	52.67.246.95	EIP reserved for NAT GW	-
InInterfaceSGId	sg-0333e92f36b2aa0bf	Security Group ID for Instances Inside Interface	-
InsideSubnetIds	subnet-047c0a2beffb5a70f	Inside subnet ID	-
InstanceSGId	sg-0c0c6bfb5ba5f1c10	Security Group ID for Instances Management Interface	-
LambdaSecurityGroupId	sg-01771b0d3012a40c5	Security Group ID for Lambda Functions	-
LambdaSubnetIds	subnet-0fb24785c687d50e4,subnet-0f1996a02ffaa2e62	List of lambda subnet IDs (comma seperated)	-
MgmtSubnetIds	subnet-02d4a757b95a9a5b9	Mangement subnet ID	-
UseGWLB	Yes	Use Gateway Load Balancer	-
VpcName	vpc-003b592ad2518d03d	Name of the VPC created	-

Étape 3 Chargez **cluster_layer.zip**, **cluster_lifecycle.zip** et **cluster_manager.zip** dans le compartiment S3 créé par **infrastructure.yaml**.

Étape 4 Déployez **deploy_asav_clustering.yaml** :

a) Allez sur **CloudFormation** et cliquez sur **Create stack** (Créer une pile); sélectionnez **With new resources (standard)** (Avec de nouvelles ressources (standard)).
b) Cliquez sur **Upload a template file** (Charger un fichier modèle), cliquez sur **Choose file** (Choisir un fichier) et sélectionnez **deploy_asav_clustering.yaml** dans le dossier cible.
c) Cliquez sur **Next** (suivant) et fournissez les informations requises.
d) Cliquez sur **Next** (Suivant), puis sur **Create stack** (Créer une pile).

Illustration 58 : Ressources déployées



Resources (21)

Search resources

Logical ID	Physical ID	Type	Status	Status reason
ASAvGroup	ran-cls-1	AWS::AutoScaling::AutoScalingGroup	CREATE_COMPLETE	-
ASAvLaunchTemplate	lt-056fd20764270c893	AWS::EC2::LaunchTemplate	CREATE_COMPLETE	-
CLSmanagerTopic	arn:aws:sns:sa-east-1:797661843114:ran-cls-1-cluster-manager-topic	AWS::SNS::Topic	CREATE_COMPLETE	-
ClusterManager	ran-cls-1-manager-lambda	AWS::Lambda::Function	CREATE_COMPLETE	-
ClusterManagerLogGrp	/aws/lambda/ran-cls-1-manager-lambda	AWS::Logs::LogGroup	CREATE_COMPLETE	-
ClusterManagerSNS1	arn:aws:sns:sa-east-1:797661843114:ran-cls-1-cluster-manager-topic:e13bfcb0-d698-4215-88a5-278474e22c32	AWS::SNS::Subscription	CREATE_COMPLETE	-
ClusterManagerSNS1Permission	ran-cls-ClusterManagerSNS1Permission-S6BQAE05OG6U	AWS::Lambda::Permission	CREATE_COMPLETE	-
InstanceEvent	ran-cls-1-notify-instance-event	AWS::Events::Rule	CREATE_COMPLETE	-
InstanceEventInvokeLambdaPermission	ran-cls-InstanceEventInvokeLambdaPermission-1XPS21Q4G2DY6	AWS::Lambda::Permission	CREATE_COMPLETE	-

L'état passe de CREATE_IN_PROGRESS à CREATE COMPLETE indiquant le déploiement réussi.

Étape 5 Vérifiez le déploiement de la grappe en vous connectant à l'un des nœuds et en saisissant la commande **show cluster info**.

```
show cluster info
```

```
Cluster oneclicktest-cluster: On
Interface mode: individual
Cluster Member Limit : 16
This is "200" in state CONTROL_NODE
ID : 0
Version : 9.19.1
Serial No.: 9AU42EN5D1E
CCL IP : 1.1.1.200
CCL MAC : 4201.0a0a.0fc7
Module : ASAv
Resource : 4 cores / 8192 MB RAM
Last join : 15:26:22 UTC Jul 17 2022
Last leave: N/A
Other members in the cluster:
Unit "204" in state DATA_NODE
ID : 1
Version : 9.19.1
Serial No.: 9AJ9N46947R
CCL IP : 1.1.1.204
CCL MAC : 4201.0a0a.0fcb
Module : ASAv
Resource : 4 cores / 8192 MB RAM
```

```
Last join : 16:57:42 UTC Jul 17 2022
Last leave: 16:03:25 UTC Jul 17 2022
```

Déployer manuellement la grappe dans AWS

Pour déployer la grappe manuellement, préparez la configuration Day0 et déployez chaque nœud.

Créer la configuration Day0 pour AWS

Fournissez la configuration de démarrage pour chaque nœud de grappe à l'aide des commandes suivantes :

Exemple d'équilibreur de charge de passerelle

Dans l'exemple suivant, une configuration en cours d'exécution est créée pour un équilibreur de charges de passerelle avec une interface Geneve pour le trafic en demi-tour et une interface VXLAN pour la liaison de commande de grappe.

```
cluster interface-mode individual force
policy-map global_policy
class inspection_default
no inspect h323 h225
no inspect h323 ras
no inspect rtsp
no inspect skinny

int m0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
no shut

interface TenGigabitEthernet0/0
nameif geneve-vtep-ifc
security-level 0
ip address dhcp
no shutdown

interface TenGigabitEthernet0/1
nve-only cluster
nameif ccl_link
security-level 0
ip address dhcp
no shutdown

interface vni1
description Clustering Interface
segment-id 1
vtep-nve 1

interface vni2
proxy single-arm
nameif ge
security-level 0
vtep-nve 2

object network ccl_link
```

```
range 10.1.90.4 10.1.90.254 //Mandatory user input, use same range on all nodes
object-group network cluster_group
network-object object ccl_link
nve 2
encapsulation geneve
source-interface geneve-vtep-ifc
nve 1
encapsulation vxlan
source-interface ccl_link
peer-group cluster_group

cluster group asav-cluster // Mandatory user input, use same cluster name on all nodes
local-unit 1 //Value in bold here must be unique to each node
cluster-interface vni1 ip 1.1.1.1 255.255.255.0 //Value in bold here must be unique to each
 node
priority 1
enable noconfirm

mtu geneve-vtep-ifc 1806
mtu ccl_link 1960
aaa authentication listener http geneve-vtep-ifc port 7575 //Use same port number on all
nodes
jumbo-frame reservation
wr mem
```

Remarque Pour les paramètres de vérification de l'intégrité d'AWS, assurez-vous de spécifier le port **aaa authentication listener http** que vous définissez ici.

Exemple d'équilibreur de charge non natif

Dans l'exemple suivant, une configuration à utiliser avec des équilibreurs de charges non natifs avec des interfaces de gestion, interne et externe est créée, ainsi qu'une interface VXLAN pour la liaison de commande de grappe.

```
cluster interface-mode individual force
interface Management0/0
management-only
nameif management
ip address dhcp

interface GigabitEthernet0/0
no shutdown
nameif outside
ip address dhcp

interface GigabitEthernet0/1
no shutdown
nameif inside
ip address dhcp

interface GigabitEthernet0/2
nve-only cluster
nameif ccl_link
ip address dhcp
no shutdown

interface vni1
description Clustering Interface
segment-id 1
```

```
vtep-nve 1

jumbo-frame reservation
mtu ccl_link 1654
object network ccl_link
range 10.1.90.4 10.1.90.254          //mandatory user input
object-group network cluster_group
network-object object ccl_link

nve 1
encapsulation vxlan
source-interface ccl_link
peer-group cluster_group

cluster group asav-cluster          //mandatory user input
local-unit 1                        //mandatory user input
cluster-interface vni1 ip 10.1.1.1 255.255.255.0  //mandatory user input
priority 1
enable
```



Remarque Si vous copiez et collez la configuration donnée ci-dessus, veillez à supprimer **//entrée utilisateur obligatoire** de la configuration.

Déployer les nœuds de la grappe

Déployez les nœuds de la grappe pour former une grappe.

Procédure

Étape 1 Déployez l'instance ASA virtuel en utilisant la configuration de jour 0 de la grappe avec le nombre d'interfaces requis (trois interfaces si vous utilisez l'équilibreur de charges de passerelle (GWLB) ou quatre interfaces si vous utilisez un équilibreur de charges non natif). Pour ce faire, dans la section **Configure Instance Details** (Configurer les détails de l'instance) > Advanced Details (détails avancés), collez la configuration du jour 0 de la grappe.

Remarque
Assurez-vous d'associer des interfaces aux instances dans l'ordre indiqué ci-dessous.

- Équilibreur de charges de passerelle AWS : trois interfaces : liaison de gestion, externe et de commande de grappe.
- Équilibreurs de charges non natifs : quatre interfaces :liaison de gestion, interne, externe et de commande de grappe.

Pour en savoir plus sur le déploiement d'ASA virtuel sur AWS, consultez Déployer l'ASA virtuel sur AWS.

Étape 2 Répétez l'étape 1 pour déployer le nombre requis de nœuds supplémentaires.

Étape 3 Utilisez la commande **show cluster info** de la console ASA virtuel pour vérifier si tous les nœuds ont bien rejoint la grappe.

Étape 4 Configurez l'équilibreur de charges de passerelle AWS

a) Créez un groupe cible et un GWLB.

b) Associez le groupe cible au GWLB.

Remarque
Assurez-vous de configurer le GWLB pour utiliser les paramètres de groupe de sécurité, de configuration d'écouteur et de vérification de l'intégrité adéquats.

c) Enregistrez l'interface de données (interface interne) avec le groupe cible à l'aide des adresses IP. Pour en savoir plus, consultez Créer un équilibreur de charges de passerelle.

Personnaliser l'opération de mise en grappe

Vous pouvez personnaliser la surveillance de l'intégrité de la mise en grappe, le délai de réplication de la connexion TCP, la mobilité des flux et d'autres optimisations, dans le cadre de la configuration day0 ou après le déploiement de la grappe.

Exécutez ces procédures sur le nœud de contrôle.

Configurer les paramètres de grappe ASA de base

Vous pouvez personnaliser les paramètres de grappe sur le nœud de contrôle.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Étape 2 (Facultatif) Activez la réplication de la console des nœuds de données vers le nœud de contrôle :

console-replicate

Par défaut, cette fonction est désactivée. L'ASA imprime certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de la console, les nœuds de données envoient les messages de la console au nœud de contrôle de sorte que vous ne devez surveiller qu'un seul port de console pour la grappe.

Étape 3 Définissez le niveau de trace minimal pour les événements de mise en grappe :

trace-level *level*

Définissez le niveau minimum comme souhaité :

- **critical**—Événements critiques (gravité=1)
- **warning**—Avertissements (gravité=2)
- **informational**—Événements informationnels (gravité=3)
- **debug**—Événements de débogage (gravité= 4)

Configurer les paramètres de surveillance de l'intégrité et de jonction automatique

Cette procédure permet de configurer la surveillance de l'intégrité des nœuds et des interfaces.

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Entrez en mode de configuration de la grappe.

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

Étape 2 Personnalisez la fonctionnalité de contrôle de l'intégrité des nœuds de la grappe.

health-check [**holdtime** *timeout*]

Pour déterminer l'intégrité des nœuds, les nœuds de la grappe ASA envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.

- **holdtime** *timeout* : détermine l'intervalle de temps entre les messages d'état de pulsation des nœuds, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver la fonctionnalité de contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées (**no health-check monitor-interface**). Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver le contrôle d'intégrité.

Exemple :

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

Étape 3 Désactivez le contrôle d'intégrité de l'interface sur une interface.

no health-check monitor-interface *interface_id*

La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Le délai avant la suppression par l'ASA d'un membre de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces. Vous pouvez le désactiver pour chaque interface en utilisant la forme **no** (non) de cette commande. Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion.

- *interface_id* : désactive la supervision d'une interface. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver la fonctionnalité de contrôle d'intégrité (**no health-check**) et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver le contrôle d'intégrité.

Exemple :

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

Étape 4 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system** : spécifie les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.
- **unlimited** : (Par défaut pour le **cluster-interface**) Ne limite pas le nombre de tentatives de jonction.
- *auto-rejoin-max* : définit le nombre de tentatives de jonction, entre 0 et 65535. **0** désactive la jonction automatique. La valeur par défaut pour les commandes **data-interface** et **system** est de 3.
- *auto_rejoin_interval* : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- *auto_rejoin_interval_variation* : définit si la durée de l'intervalle augmente. Définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données et le système.

Exemple :

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

Étape 5 Configurez le délai antirebond avant que l'ASA considère une interface comme défaillante et que le nœud ne soit supprimé de la grappe.

health-check monitor-interface debounce-time *ms*

Exemple :

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

Définissez le délai antirebond entre 300 et 9 000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai

antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe.

Étape 6 (Facultatif) Configurez la surveillance de la charge de trafic.

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* : définit le délai en secondes entre les messages de surveillance, entre 10 et 360 secondes. La valeur par défaut est de 20 secondes.
- **intervals** *intervals* : définit le nombre d'intervalles pour lesquels l'ASA conserve les données, entre 1 et 60. La valeur par défaut est 30.

Vous pouvez superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud si les nœuds restants peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Vous pouvez superviser périodiquement la charge de trafic. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud.

Utilisez la commande **show cluster info load-monitor** pour afficher la charge de trafic.

Exemple :

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

Exemple

L'exemple suivant configure le délai de rétention du contrôle d'intégrité à 0,3 seconde; désactive la surveillance sur l'interface Management 0/0; définit la reconnexion automatique pour les interfaces de données à 4 tentatives commençant à 2 minutes, en multipliant la durée de 3 fois l'intervalle précédent; et définit la reconnexion automatique pour la liaison de commande de grappe à 6 tentatives toutes les 2 minutes.

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

Gérer les nœuds de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les nœuds de cette dernière.

Devenir un nœud inactif

Pour devenir un membre inactif de la grappe, désactivez la mise en grappe sur le nœud tout en laissant intacte la configuration de mise en grappe.

Remarque Lorsqu'un ASA devient inactif (soit manuellement, soit à la suite d'un échec du contrôle d'intégrité), toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe; ou vous pouvez supprimer complètement le nœud de la grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), alors l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Procédure

Étape 1 Entrez en mode de configuration de la grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 2 Désactivez la mise en grappe :

no enable

Si ce nœud était le nœud de contrôle, une nouvelle sélection de contrôle a lieu et un autre membre devient le nœud de contrôle.

La configuration de la grappe est conservée, vous pouvez donc réactiver la mise en grappe ultérieurement.

Désactiver un nœud de données à partir du nœud de contrôle

Pour désactiver un membre autre que le nœud auquel vous êtes connecté, effectuez les étapes suivantes.

Remarque Lorsqu'un ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Procédure

Supprimez le nœud de la grappe.

cluster remove unit *node_name*

La configuration de démarrage reste inchangée, ainsi que la dernière configuration synchronisée à partir du nœud de contrôle, afin que vous puissiez rajouter le nœud ultérieurement sans perdre votre configuration. Si vous saisissez cette commande sur un nœud de données pour supprimer le nœud de contrôle, un nouveau nœud de contrôle est élu.

Pour afficher les noms des membres, saisissez **cluster remove unit ?**, ou saisissez la commande **show cluster info**.

Exemple :

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement un membre, vous devez rejoindre manuellement la grappe.

Procédure

Étape 1 Sur la console, passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 2 Activez la mise en grappe.

enable

Quitter la grappe

Si vous souhaitez quitter complètement la grappe, vous devez supprimer toute la configuration de démarrage de la grappe. Étant donné que la configuration actuelle sur chaque nœud est la même (synchronisée à partir de l'unité active), quitter la grappe implique également de restaurer une configuration antérieure à la grappe à partir d'une sauvegarde ou d'effacer votre configuration et de recommencer pour éviter les conflits d'adresses IP.

Procédure

Étape 1 Pour un nœud de données, désactivez la mise en grappe :

cluster group *cluster_name* **no enable**

Exemple :

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

Vous ne pouvez pas modifier la configuration lorsque la mise en grappe est activée sur un nœud de données.

Étape 2 Effacez la configuration de la grappe :

clear configure cluster

L'ASA désactive toutes les interfaces, y compris l'interface de gestion et la liaison de commande de grappe.

Étape 3 Désactivez le mode d'interface de la grappe :

no cluster interface-mode

Le mode n'est pas stocké dans la configuration et doit être réinitialisé manuellement.

Étape 4 Si vous avez une configuration de sauvegarde, copiez-la dans la configuration en cours d'exécution :

copy *backup_cfg* **running-config**

Exemple :

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

Étape 5 Enregistrez la configuration pour le démarrage :

write memory

Étape 6 Si vous n'avez pas de configuration de sauvegarde, reconfigurez l'accès de gestion. Par exemple, assurez-vous de modifier les adresses IP de l'interface et de restaurer le bon nom d'hôte.

Modifier le nœud de contrôle

⚠

Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez spécifier le nœud exact que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez toutefois que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle à l'aide de cette procédure, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Procédure

Définissez un nouveau nœud comme nœud de contrôle :

cluster control-node unit*node_name*

Exemple :

```
ciscoasa(config)# cluster control-node unit asa2
```

Vous devrez vous reconnecter à l'adresse IP de la grappe principale.

Pour afficher les noms des membres, saisissez **cluster control-node unit ?** (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exécuter une commande à l'échelle de la grappe

Pour envoyer une commande à tous les nœuds de la grappe ou à un nœud en particulier, procédez comme suit. L'envoi d'une commande **show** à tous les nœuds collecte toutes les sorties et les affiche sur la console du nœud actuel. D'autres commandes, telles que **capture** et **copy**, peuvent également profiter d'une exécution à l'échelle de la grappe.

Procédure

Envoyez une commande à tous les nœuds ou, si vous spécifiez le nom du nœud, à un nœud en particulier :

cluster exec [**unit** *node_name*] *command*

Exemple :

```
ciscoasa# cluster exec show xlate
```

Pour afficher les noms de nœud, saisissez **cluster exec unit ?** (unité d'exécution de grappe?) (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exemples

Pour copier simultanément le même fichier de capture de tous les nœuds de la grappe vers un serveur TFTP, saisissez la commande suivante sur le nœud de contrôle :

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Plusieurs fichiers PCAP, un pour chaque nœud, sont copiés sur le serveur TFTP. Le nom du fichier de capture de destination est automatiquement associé au nom du nœud, par exemple capture1_asa1.pcap, capture1_asa2.pcap, etc. Dans cet exemple, asa1 et asa2 sont des noms de nœuds de grappe.

Surveillance de la grappe

Vous pouvez superviser et dépanner l'état de la grappe et les connexions.

Supervision de l'état de la grappe

Consultez les commandes suivantes pour superviser l'état de la grappe :

- **show cluster info** [**health** [**details**]]

  En l'absence de mot clé, la commande **show cluster info** affiche l'état de tous les membres de la grappe.

  La commande **show cluster info health** affiche l'intégrité actuelle des interfaces, des nœuds et de la grappe dans son ensemble. Le mot clé **details** affiche le nombre d'échecs de messages de pulsation.

  Consultez la sortie suivante pour la commande **show cluster info** :

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
```

```
Unit "D" in state DATA_NODE
    ID        : 1
    Site ID   : 1
          Version   : 9.4(1)
    Serial No.: P3000000001
    CCL IP    : 10.0.0.4
    CCL MAC   : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2011
    Last leave: N/A
Unit "A" in state CONTROL_NODE
    ID        : 2
    Site ID   : 2
          Version   : 9.4(1)
    Serial No.: JAB0815R0JY
    CCL IP    : 10.0.0.1
    CCL MAC   : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2011
    Last leave: N/A
Unit "B" in state DATA_NODE
    ID        : 3
    Site ID   : 2
          Version   : 9.4(1)
    Serial No.: P3000000191
    CCL IP    : 10.0.0.2
    CCL MAC   : 000b.fcf8.c61e
    Last join : 19:13:50 UTC Sep 23 2011
    Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  Indique si le nœud de la grappe rejoindra automatiquement la grappe après un délai et si les conditions de défaillance (comme l'attente de la licence, l'échec de la vérification de l'intégrité du châssis, etc.) sont supprimées. Si le nœud est désactivé de façon permanente ou si le nœud est déjà dans la grappe, cette commande n'affichera aucune sortie.

  Consultez les sorties suivantes pour la commande **show cluster info auto-join** :

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
```

```
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport** {**asp** | **cp** [**detail**]}

  Affiche les statistiques relatives au transport pour les éléments suivants :

  - **asp** – Statistiques de transport du plan de données.
  - **cp** – Statistiques de transport du plan de commande.

    Si vous saisissez le mot clé **detail**, vous pouvez afficher l'utilisation du protocole de transport fiable de la grappe afin de cerner les problèmes d'abandon de paquet lorsque le tampon est plein dans le plan de commande. Consultez la sortie suivante pour la commande **show cluster info transport cp detail** :

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
--------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
```

```
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%
```

```
Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                       578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                       572         99%
  Cluster VPN Unique ID Client                     1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  Affiche l'historique de la grappe, ainsi que les messages d'erreur indiquant pourquoi un nœud de grappe n'a pas pu se joindre ou pourquoi un nœud a quitté a grappe.

Capture des paquets à l'échelle de la grappe

Consultez la commande suivante pour capturer des paquets dans une grappe :

cluster exec capture

Pour prendre en charge le dépannage à l'échelle de la grappe, vous pouvez activer la capture du trafic spécifique à la grappe sur le nœud de contrôle à l'aide de la commande **cluster exec capture**, qui est ensuite automatiquement activée sur tous les nœuds de données de la grappe.

Supervision des ressources de la grappe

Consultez la commande suivante pour surveiller les ressources de la grappe :

show cluster {**cpu** | **memory** | **resource**} [*options*]

Affiche les données agrégées pour l'ensemble de la grappe. Les *options* disponibles dépendent du type de données.

Supervision du trafic de la grappe

Consultez les écrans suivantes pour superviser le trafic de la grappe :

- **show conn [detail], cluster exec show conn**

  La commande **show conn** indique si un flux est un flux de directeur, de sauvegarde ou de transfert. Utilisez la commande **cluster exec show conn** sur n'importe quel nœud pour afficher toutes les connexions. Cette commande peut montrer comment le trafic d'un flux unique arrive à différents ASA dans la grappe. Le débit de la grappe dépend de l'efficacité et de la configuration de l'équilibrage de charges. Cette commande offre un moyen simple d'afficher le trafic d'une connexion dans la grappe et peut vous aider à comprendre comment un équilibreur de charges peut affecter les performances d'un flux.

  La commande **show conn detail** indique également quels flux sont soumis à la mobilité des flux.

  L'exemple suivant illustre une sortie de la commande **show conn detail** :

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic received
 at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface NP
Identity
Ifc Locally received: 716 (8 byte/s)
```

Pour dépanner le flux de connexion, observez d'abord les connexions sur tous les nœuds en saisissant la commande **cluster exec show conn** sur n'importe quel nœud. Recherchez les flux qui ont les indicateurs suivants : directeur (Y), sauvegarde (y) et transitaire (z). L'exemple suivant montre une connexion SSH de 172.18.124.187:22 à 192.168.103.131:44727 sur les trois ASA; l'ASA 1 a l'indicateur z indiquant qu'il s'agit d'un transitaire pour la connexion, l'ASA 3 a l'indicateur y indiquant qu'il est le directeur de la connexion et l'ASA 2 n'a pas d'indicateurs spéciaux indiquant qu'il est le propriétaire. Dans le sens sortant, les paquets de cette connexion pénètrent dans l'interface interne de l'ASA 2 et quittent l'interface externe. Dans le sens entrant, les paquets de cette connexion pénètrent dans l'interface externe sur l'ASA 1 et l'ASA 3, sont acheminés sur la liaison de commande de grappe vers l'ASA 2, puis quittent l'interface interne sur l'ASA 2.

```
ciscoasa/ASA1/control node# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**********************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**********************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  Les commandes **show cluster info conn-distribution** et **show cluster info packet-distribution** affichent la distribution du trafic sur tous les nœuds de la grappe. Ces commandes peuvent vous aider à évaluer et à ajuster l'équilibreur de charges externe.

  La commande **show cluster info loadbalance** affiche les statistiques de rééquilibrage des connexions.

  La commande **show cluster info flow-mobility counters** affiche les renseignements sur le mouvement de l'EID et le mouvement du propriétaire du flux. Consultez la sortie suivante pour **show cluster info flow-mobility counters** :

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  La commande **show cluster info load-monitor** affiche la charge de trafic pour les membres de la grappe pour le dernier intervalle ainsi que la moyenne du nombre total d'intervalles configurés (30 par défaut). Utilisez le mot clé **details** pour afficher la valeur de chaque mesure à chaque intervalle.

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
```

```
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 30 interval:
   0           0            0            12             28
   1           0            0            13             27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval



Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0
```

```
         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Memory usage(%) captured over 30 intervals:

Unit ID  0

        25         25         30         30         30         35

        25         25         35         30         30         30

        25         25         30         25         25         35

        30         30         30         25         25         25

        25         20         30         30         30         30

Unit ID  1

        30         25         35         25         30         30

        25         25         35         25         30         35

        30         30         35         30         30         30

        25         20         30         25         25         30

        20         30         35         30         30         35


CPU usage(%) captured over 30 intervals:

Unit ID  0

        25         25         30         30         30         35

        25         25         35         30         30         30

        25         25         30         25         25         35

        30         30         30         25         25         25

        25         20         30         30         30         30

Unit ID  1

        30         25         35         25         30         30

        25         25         35         25         30         35
```

```
        30          30          35          30          30          30

        25          20          30          25          25          30

        20          30          35          30          30          35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity | xlate**} [*options*]

  Affiche les données agrégées pour l'ensemble de la grappe. Les *options* disponibles dépendent du type de données.

  Consultez la sortie suivante pour la commande **show cluster access-list** :

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

  Pour afficher le nombre agrégé des connexions utilisées pour tous les nœuds, saisissez :

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used

  cl1:*************************************************************
```

```
  100 in use, 100 most used
```

- **show asp cluster counter**

  Cette commande est utile pour le dépannage des chemins de données.

Supervision du routage de la grappe

Consultez les commandes suivantes pour le routage de la grappe :

- **show route cluster**
- **debug route cluster**

  Affiche les renseignements sur la grappe pour le routage.

- **show lisp eid**

  Affiche le tableau EID de l'ASA qui indique les EID et les ID de site.

  Consultez la sortie suivante de la commande **cluster exec show lisp eid**.

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):**************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:**************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  Cette commande est utile pour la résolution de problèmes.

Configuration de la journalisation pour la mise en grappe

Consultez la commande suivante pour configurer la journalisation pour la mise en grappe :

logging device-id

Chaque nœud de la grappe génère des messages de journal système de manière indépendante. Vous pouvez utiliser la commande **logging device-id** pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant de nœuds identiques ou différents dans la grappe.

Supervision des interfaces de grappe

Consultez les commandes suivantes pour superviser les interfaces de la grappe :

- **show cluster interface-mode**

  Affiche le mode d'interface de la grappe.

Débogage de la mise en grappe

Consultez les commandes suivantes pour le débogage de la mise en grappe :

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  Affiche les messages de débogage pour la mise en grappe.

- **debug cluster flow-mobility**

  Affiche les événements liés à la mobilité des flux de mise en grappe.

- **debug lisp eid-notify-intercept**

  Affiche les événements lorsque le message eid-notify est intercepté.

- **show cluster info trace**

  La commande **show cluster info trace** affiche les renseignements de débogage pour un dépannage ultérieur.

  Consultez la sortie suivante pour la commande **show cluster info trace** :

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

  Par exemple, si vous voyez les messages suivants indiquant que deux nœuds ayant le même nom **local-unit** agissent en tant que nœud de contrôle, cela peut signifier que deux nœuds ont le même nom **local-unit** (vérifiez votre configuration) ou qu'un nœud reçoit ses propres messages de diffusion (vérifiez votre réseau).

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node
 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe de l'ASA

Certaines fonctionnalités d'ASA ne sont pas prises en charge avec la mise en grappe d'ASA, et d'autres le sont uniquement sur le nœud de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

- Fonctionnalités de communication unifiée qui reposent sur le mandataire TLS
- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Interfaces de tunnel virtuel (VTI)
- Les inspections d'application suivantes :
  - CTIQBE
  - H323, H225 et RAS
  - Intercommunication IPsec
  - MGCP
  - MMP
  - RTSP
  - SCCP (Skinny)
  - WAAS
  - WCCP
- Filtre de trafic de réseau de zombies
- Auto Update Server
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Équilibrage de la charge VPN
- Basculement
- Routage et pont intégrés
- Mode FIPS

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.

Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET
  - SunRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique
- Autorisation et authentification pour l'accès réseau La comptabilité est décentralisée.
- Services de filtrage
- VPN de site à site
- Routage multidiffusion

Fonctionnalités appliquées aux nœuds individuels

Ces fonctionnalités sont appliquées à chaque nœud ASA, plutôt qu'à la grappe dans son ensemble ou au nœud de contrôle.

- QoS : la politique QoS est synchronisée dans la grappe dans le cadre de la duplication de la configuration. Cependant, la politique est appliquée sur chaque nœud indépendamment. Par exemple, si vous configurez le contrôle en sortie, les valeurs de débit de conformité et de rafale de conformité s'appliquent au trafic sortant d'un ASA particulier. Dans une grappe à 3 nœuds et avec le trafic réparti uniformément, le taux de conformité devient en fait trois fois supérieur au débit de la grappe.

- Détection des menaces : la détection des menaces fonctionne sur chaque nœud indépendamment; par exemple, les statistiques principales sont propres au nœud. La détection de l'analyse de port, par exemple, ne fonctionne pas, car l'analyse du trafic sera équilibrée entre tous les nœuds et un nœud ne verra pas tout le trafic.

AAA pour l'accès réseau et la mise en grappe

L'AAA pour l'accès réseau comprend trois composants : l'authentification, l'autorisation et la gestion de comptes. L'authentification et l'autorisation sont mises en œuvre en tant que fonctionnalités centralisées sur le nœud de contrôle de mise en grappe avec la duplication des structures de données sur les nœuds de données de grappe. Si un nœud de contrôle est choisi, le nouveau nœud de contrôle disposera de toute l'information nécessaire pour continuer le fonctionnement ininterrompu des utilisateurs authentifiés établis et de leurs autorisations associées. Les délais d'inactivité et absolue pour l'authentification des utilisateurs sont conservés lors d'un changement de nœud de contrôle se produit.

La comptabilité est mise en œuvre en tant que fonctionnalité distribuée dans une grappe. La comptabilité est effectuée flux par flux, de sorte que le nœud de la grappe possédant un flux enverra les messages de démarrage et d'arrêt de comptabilité au serveur AAA lorsque la comptabilité est configurée pour un flux.

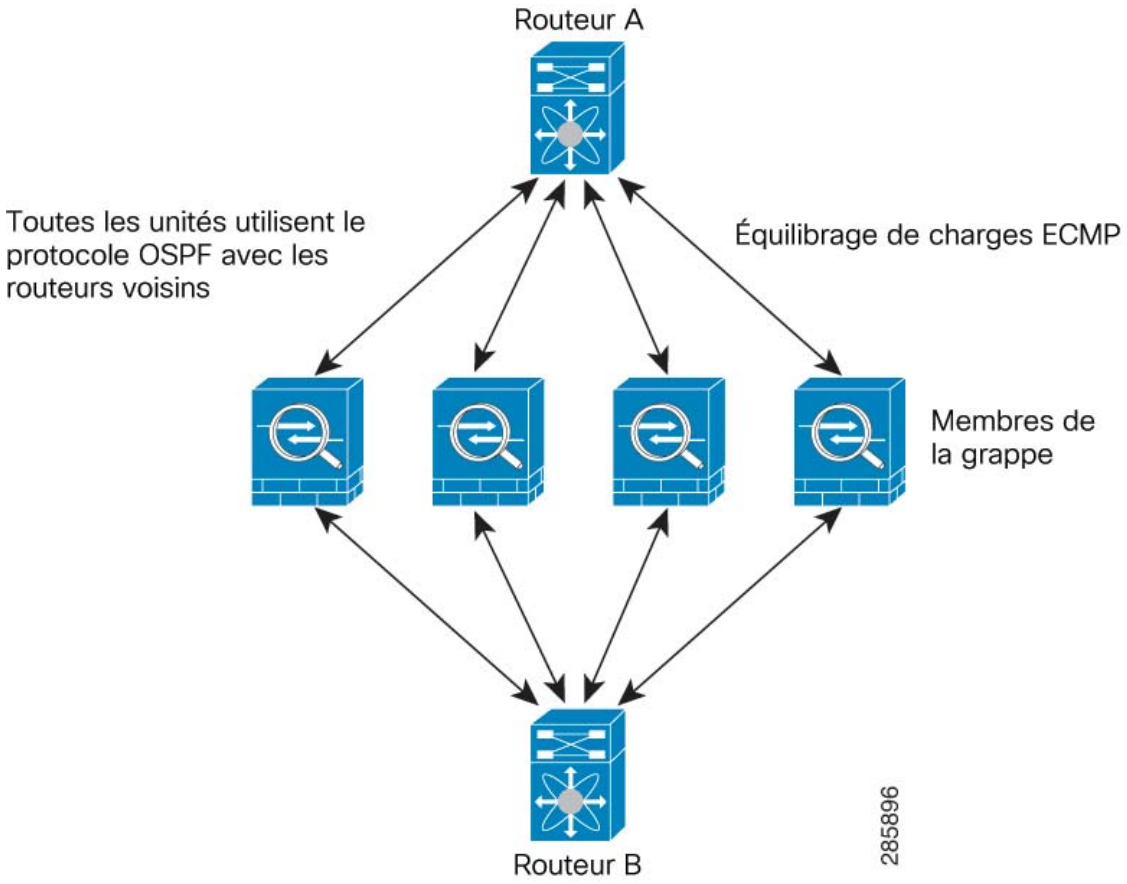
Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe (voir les commandes **set connection conn-max**, **set connection embryonic-conn-max**, **set connection per-client-embryonic-max**, et **set connection per-client-max**). Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

Routage et mise en grappe dynamiques

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 59 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Remarque Si la grappe comporte plusieurs contiguïtés avec le même routeur à des fins de redondance, le routage dissymétrique peut entraîner une perte de trafic inacceptable. Pour éviter le routage dissymétrique, regroupez toutes ces interfaces de nœud dans la même zone de trafic. Voir Configurer une zone de trafic, à la page 822.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le

propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.

- Si vous utilisez l'AAA pour l'accès FTP, le flux du canal de contrôle est centralisé sur le nœud de contrôle.

Inspection ICMP et mise en grappe

Le flux des paquets d'erreurs ICMP et ICMP dans la grappe varie selon que l'inspection d'erreurs ICMP ou ICMP est activée ou non. Sans inspection ICMP, ICMP est un flux unidirectionnel et il n'y a pas de prise en charge de flux directeur. Avec l'inspection ICMP, le flux ICMP devient bidirectionnel et est soutenu par un flux directeur/de sauvegarde. L'une des différences avec un flux ICMP inspecté réside dans le traitement par le directeur du paquet transféré : le directeur transmettra le paquet de réponse d'écho ICMP au propriétaire du flux au lieu de retourner le paquet au transitaire.

Routage multidiffusion et mise en grappe

En mode d'interface individuel, les unités n'agissent pas indépendamment avec la multidiffusion. Toutes les données et les paquets de routage sont traités et transmis par l'unité de contrôle, évitant ainsi la duplication des paquets.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents ASAdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à ASA qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- No Proxy ARP (Pas de serveur mandataire ARP) : pour les interfaces individuelles, une réponse de serveur mandataire ARP n'est jamais envoyée pour les adresses mappées. Cela empêche le routeur adjacent de maintenir une relation d'homologue avec un ASA qui ne fait plus partie de la grappe. Le routeur en amont a besoin d'une route statique ou d'un PBR avec suivi d'objets pour les adresses mappées qui pointe vers l'adresse IP de la grappe principale. Ce n'est pas un problème pour un EtherChannel étendu, car il n'y a qu'une seule adresse IP associée à l'interface de grappe.

- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :

  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.

  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.

  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un

problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.

- Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.

- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, la grappe divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.

- Réutiliser un pool PAT dans plusieurs règles : pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.

- Pas de tourniquet : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.

- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.

- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.

- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.

- Fonctionnalité PAT par session : bien qu'elle ne soit pas exclusive à la mise en grappe, la fonctionnalité PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque nœud de données de posséder des connexions PAT; en revanche, les connexions PAT multisessions doivent être transférées au nœud de contrôle et détenues par celui-ci. Par défaut, tout le trafic TCP et le trafic DNS UDP utilisent un xlate PAT par session, tandis que ICMP et tout le reste du trafic UDP utilise la multisession. Vous pouvez configurer des règles NAT par session pour modifier ces valeurs par défaut pour TCP et UDP, mais vous ne pouvez pas configurer la PAT par session pour ICMP. Par exemple, en raison de l'utilisation croissante du protocole Quic sur le port UDP/443 comme alternative de performance à HTTPS TLS sur TCP/443, vous devriez activer la traduction d'adresses par session (PAT) pour UDP/443. Pour le trafic qui bénéficie de la PAT multisession, comme le H.323, le SIP ou l'interface simplifiée, vous pouvez désactiver la PAT par session pour les ports TCP associés (les ports UDP de ces ports H.323 et SIP sont déjà multisession en par défaut). Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

SCTP et mise en grappe

Une association SCTP peut être créée sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses connexions multi-hébergement doivent résider sur le même nœud.

Inspection SIP et mise en grappe

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

La configuration du mandataire TLS n'est pas prise en charge.

SNMP et mise en grappe

Un agent SNMP interroge chaque ASA en fonction de l'adresse IP locale de son . Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud.Vous devez les rajouter sur le nœud de contrôle pour forcer les utilisateurs à se reproduire vers le nouveau nœud, ou directement sur le nœud de données.

STUN et mise en grappe

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Syslog et mise en grappe

- Syslog : chaque nœud de la grappe génère ses propres messages de journal système. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.
- NetFlow : chaque nœud de la grappe génère son propre flux NetFlow. Le collecteur NetFlow peut traiter chaque appareil ASA uniquement comme un exportateur NetFlow distinct.

Cisco Trustsec et mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; seul le nœud de contrôle prend en charge les connexions VPN.

Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Pour les connexions à une interface individuelle lors de l'utilisation de PBR ou d'ECMP, vous devez toujours vous connecter à l'adresse IP de la grappe principale, et non à une adresse locale.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

Choix du nœud de contrôle

Les nœuds de la grappe communiquent sur la liaison de commande de grappe pour élire un nœud de contrôle comme suit :

1. Lorsque vous activez la mise en grappe pour un nœud (ou lorsqu'il démarre avec la mise en grappe déjà activée), il diffuse une demande de sélection toutes les 3 secondes.
2. Tous les autres nœuds ayant une priorité plus élevée répondent à la demande de sélection; la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.



Remarque Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud se joint ultérieurement à la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle; le nœud de contrôle existant demeure toujours le nœud de contrôle, sauf s'il s'arrête de répondre, moment auquel un nouveau nœud de contrôle est sélectionné.
5. Dans un scénario de « discernement partagé », où il y a temporairement plusieurs nœuds de contrôle, le nœud ayant la priorité la plus élevée conserve le rôle tandis que les autres nœuds retournent aux rôles de nœud de données.



Remarque Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

Surveillance de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

Lorsque vous activez la surveillance de l'intégrité, toutes les interfaces physiques sont supervisées par défaut; vous pouvez éventuellement désactiver la surveillance par interface. Seules les interfaces nommées peuvent être surveillées.

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le délai avant la suppression par l'ASA d'un membre de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. L'ASA ne supervise pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de l'ASA de la grappe. Le nœud est supprimé après 500 ms, quel que soit son état.

État après l'échec

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

ASA tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.



Remarque Lorsque ASA devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Rejoindre la grappe

Après le retrait d'un nœud de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe au niveau de l'interface de ligne de commande en saisissant la commande **cluster group** *name*, puis **enable**.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : l'ASA essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment. Ce comportement est configurable.
- Échec de l'interface de données : l'ASA tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'ASA désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe au niveau de l'interface de ligne de commande en saisissant la commande **cluster group** *name*, puis **enable**. Ce comportement est configurable.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que la liaison de commande de grappe soit active et que la mise en grappe soit toujours activée avec la commande **enable**. L'ASA tente de rejoindre la grappe toutes les 5 secondes.

- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc. Un nœud tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Ce comportement est configurable.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 22 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
Tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	Comprend les règles AAA (uauth).
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—
VPN distribué (site à site) pour Firepower 4100/9300	Oui	La session de sauvegarde devient la session active, puis une nouvelle session de sauvegarde est créée.

Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.

- Propriétaire du sauvegarde : nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis.

  Si vous activez la localisation du directeur pour la mise en grappe inter-sites, il existe deux rôles de propriétaire de la sauvegarde : le rôle de sauvegarde locale et de sauvegarde globale. Le propriétaire choisit toujours une sauvegarde locale sur le même site que lui (en fonction de l'ID du site). La sauvegarde globale peut se trouver sur n'importe quel site et peut même se trouver sur le même nœud que la sauvegarde locale. Le propriétaire envoie des informations sur l'état de la connexion aux deux sauvegardes.

  Si vous activez la redondance de sites et que le propriétaire de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La sauvegarde de châssis et la sauvegarde de site sont indépendantes. Par conséquent, dans certains cas, un flux comportera à la fois une sauvegarde de châssis et une sauvegarde de site.

- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Si vous activez la localisation de directeur pour la mise en grappe inter-sites, il y a deux rôles de directeur : le directeur local et le directeur global. Le propriétaire choisit toujours un directeur local sur le même site que lui (en fonction de l'ID du site). Le directeur global peut être sur n'importe quel site et peut même être le même nœud que le directeur local. En cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site.

  Détails du hachage ICMP/ICMPv6 :

  - Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
  - Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
  - Pour les autres paquets, les ports source et de destination sont à 0.

- Transitaire : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Si vous activez la localisation de directeur, le redirecteur interroge toujours le directeur local. Le transitaire n'interroge le directeur global que si le directeur local ne connaît pas le propriétaire, par exemple, si un membre de la grappe reçoit des paquets pour une connexion qui appartient à un autre site. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.

Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- Propriétaire de fragment : pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Connexions par traduction d'adresse de port

Lorsqu'une connexion utilise la traduction d'adresses de port (PAT), le type de PAT (par session ou multisession) influence quel membre de la grappe devient propriétaire de la nouvelle connexion :

- PAT par session : le propriétaire est le nœud qui reçoit le paquet initial dans la connexion.

  Par défaut, le trafic TCP et DNS UDP utilise une PAT par session.

- PAT multisession : le propriétaire est toujours le nœud de contrôle. Si une connexion PAT multisession est initialement reçue par un nœud de données, le nœud de données transfère la connexion au nœud de contrôle.

  Par défaut, le trafic UDP (à l'exception du trafic UDP DNS) et ICMP utilise la PAT multisession. Ces connexions appartiennent donc toujours au nœud de contrôle.

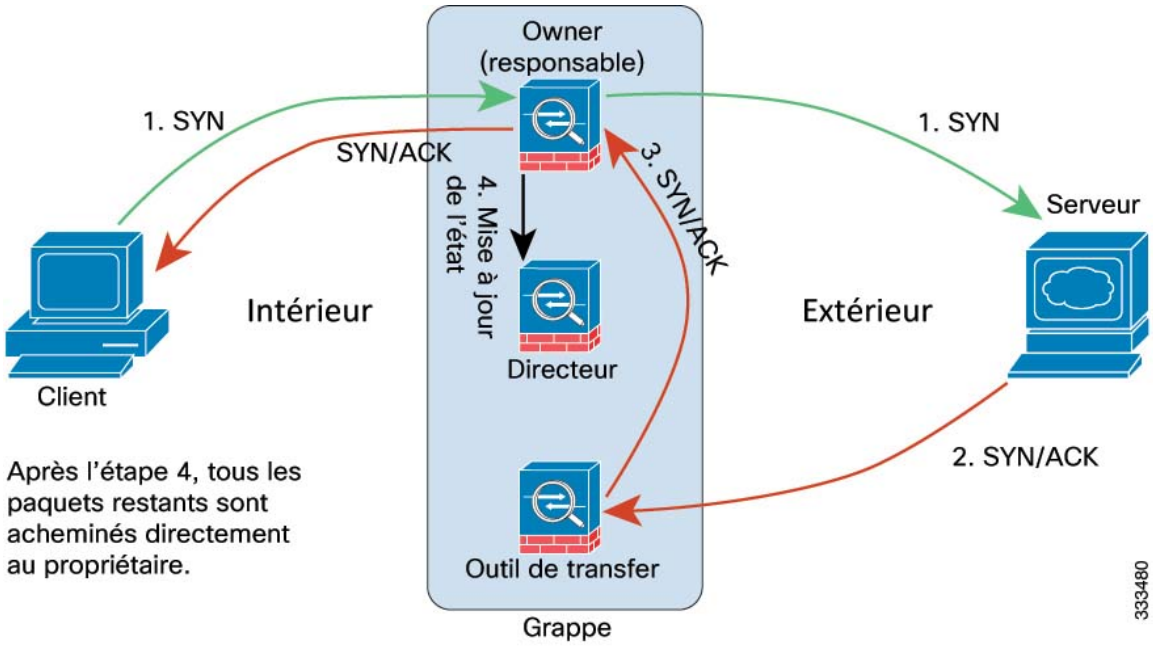
Vous pouvez modifier les valeurs par défaut de PAT par session pour les protocoles TCP et UDP afin que les connexions à ces protocoles soient gérées par session ou multisession selon la configuration. Pour ICMP, vous ne pouvez pas modifier la PAT multisession par défaut. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Pour de meilleures performances, un bon équilibrage de la charge externe est nécessaire pour que les deux directions d'un flux arrivent au même nœud et pour que les flux soient répartis uniformément entre les nœuds. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.



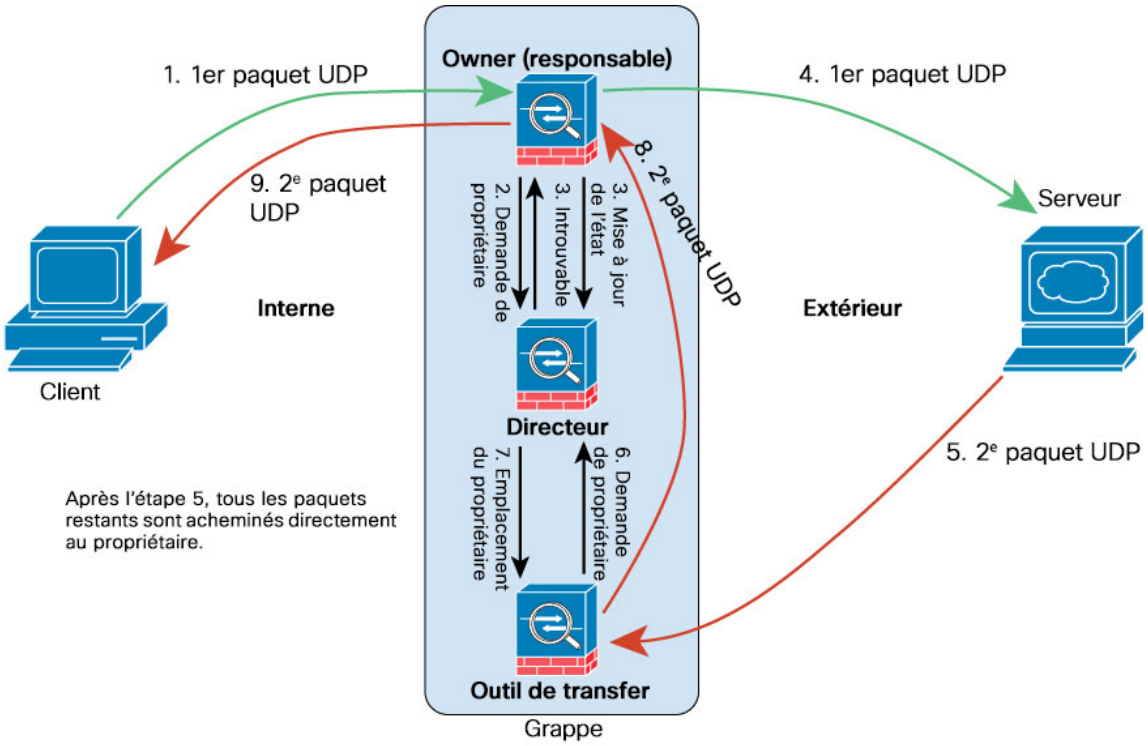
1. Le paquet SYN provient du client et est livré à un ASA (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un ASA différent (selon la méthode d'équilibrage de la charge). Cet ASA est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.
5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.

7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. ***Illustration 60 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un ASA (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.
6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.

8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Historique de la mise en grappe d'ASA virtuel dans le nuage public

Fonctionnalités	Version	Détails
Mise en grappe d'ASA virtuel sur Amazon Web Services (AWS)	9.19(1)	L'ASA virtuel prend en charge la mise en grappe d'interfaces individuelles pour un maximum de 16 nœuds sur AWS. Vous pouvez utiliser la mise en grappe avec ou sans équilibreur de charge de la passerelle AWS.



PARTIE III

Interfaces

- Configuration de l'interface de base, à la page 671
- Configuration de base de l’interface pour les ports de commutation du Firepower 1010, à la page 689
- Interfaces EtherChannel , à la page 707
- Interfaces de boucle avec retour, à la page 721
- Sous-interfaces VLAN, à la page 727
- Interfaces VXLAN, à la page 735
- Interfaces en mode routage et en mode transparent, à la page 763
- Configuration avancée de l'interface, à la page 803
- Zones de circulation, à la page 813



CHAPITRE 14

Configuration de l'interface de base

Ce chapitre comprend la configuration de l'interface de base, y compris les paramètres Ethernet et la configuration de la trame étendue.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution système, saisissez la commande **changeto system.** .

Remarque Pour Firepower 2100 en mode plateforme et Châssis Firepower 4100/9300 , vous devez configurer les paramètres de l'interface de base dans le système d'exploitation FXOS. Consultez le guide de configuration ou de démarrage de votre châssis pour en savoir plus.

- À propos de la configuration de l'interface de base, à la page 671
- Lignes directrices pour la configuration de l'interface de base, à la page 674
- Paramètres par défaut pour la configuration de l'interface de base, à la page 674
- Activer l'interface physique et configurer les paramètres Ethernet, à la page 675
- Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 678
- Gérer le module de réseau pour Cisco Secure Firewall, à la page 679
- Surveillance des interfaces, à la page 684
- Exemples d'interfaces de base, à la page 684
- Historique de la configuration de l'interface de base, à la page 685

À propos de la configuration de l'interface de base

Cette section décrit les fonctionnalités de l'interface et les interfaces spéciales.

Fonctionnalité Auto-MDI/MDIX

Pour les interfaces RJ-45, le paramètre de négociation automatique par défaut inclut également la fonction Auto-MDI/MDIX. La fonction Auto-MDI/MDIX élimine le besoin de câblage croisé en effectuant un croisé interne lorsqu'un câble droit est détecté pendant la phase de négociation automatique. La vitesse ou le duplex doivent être réglés pour qu'ils soient négociés automatiquement afin d'activer Auto-MDI/MDIX pour l'interface.

Si vous définissez explicitement la vitesse et le duplex à une valeur fixe, désactivant ainsi la négociation automatique pour les deux paramètres, Auto-MDI/MDIX est également désactivé. Pour Gigabit Ethernet, lorsque la vitesse et le mode duplex sont définis à 1000 et plein, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

Interface de gestion

L'interface de gestion, selon votre modèle, est une interface distincte réservée au trafic de gestion.

Présentation de l'interface de gestion

Vous pouvez gérer l'ASA en vous connectant à :

- Toute interface de trafic entrant
- Une interface *logement*/*port* de gestion dédiée (si disponible pour votre modèle)

Vous devrez peut-être configurer l'accès de gestion à l'interface en fonction de l'Accès de gestion, à la page 1275.

L'interface de *logement*/*port* de gestion

Le tableau suivant présente les interfaces de gestion par modèle.

Tableau 23 : Interfaces de gestion par modèle

Modèle	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable pour le trafic de transit	Sous-interfaces autorisées
Firepower 1000	—	—	—	**Oui**	**Oui**	**Oui**
Firepower de la série 2100	—	—	—	**Oui**	— **Remarque :** techniquement, vous pouvez activer le trafic de transit; toutefois, le débit de cette interface n'est pas suffisant pour les opérations de données.	**Oui**
Secure Firewall 3100	—	—	—	**Oui**	**Oui**	**Oui**

Modèle	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable pour le trafic de transit	Sous-interfaces autorisées
Firepower 4100/9300	S. O. L'ID d'interface dépend de l'interface physique de type gestion que vous avez attribuée au périphérique logique ASA	—	—	—	—	**Oui**
ISA 3000	—	—	—	**Oui**	—	—
ASAv	**Oui**	—	—	—	**Oui**	—

Utiliser n'importe quelle interface pour le trafic de gestion uniquement

Vous pouvez utiliser n'importe quelle interface comme interface de gestion uniquement en la configurant pour le trafic de gestion, y compris une interface EtherChannel (voir la commande **management-only**).

Interface de gestion pour le mode transparent

En mode de pare-feu transparent, en plus du nombre maximum d'interfaces de trafic autorisé, vous pouvez également utiliser l'interface de gestion (l'interface physique ou une sous-interface (si prise en charge par votre modèle)) en tant qu'interface de gestion distincte uniquement.

Vous ne pouvez pas utiliser d'autres types d'interfaces comme interfaces de gestion.

Pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA.

Remarque L'interface de gestion ne fait pas partie d'un groupe de ponts normal. Notez que pour des raisons opérationnelles, elle fait partie d'un groupe de ponts non configurable.

Trafic de gestion uniquement

L'interface de gestion traite uniquement le trafic entrant et sortant et ne peut pas transmettre de trafic de transit. Dans tous les cas, comme les groupes de ponts ne peuvent pas communiquer avec d'autres groupes de ponts, il serait impossible à l'interface de gestion d'acheminer vers un groupe de ponts, ou inversement, même si elle prenait en charge le trafic.

Tableau d'adresses MAC partagées et connexions de commutateurs

En mode de pare-feu transparent, l'interface de gestion met à jour le tableau d'adresses MAC de l'ASA de la même manière qu'une interface de données; par conséquent, vous ne devez pas connecter à la fois une interface de gestion et une interface de données au même commutateur, sauf si vous configurez l'un des ports de commutation en tant que port routé (par défaut, les commutateurs Catalyst partagent une adresse MAC pour

tous les ports de commutation VLAN). Sinon, si le trafic arrive sur l'interface de gestion à partir du commutateur physiquement connecté, l'ASA met à jour le tableau d'adresses MAC pour utiliser l'interface de *gestion* pour accéder au commutateur, au lieu de l'interface de données. Cette action entraîne une interruption temporaire du trafic; pour des raisons de sécurité, l'ASA ne mettra pas à jour le tableau d'adresses MAC pour les paquets du commutateur vers l'interface de données pendant au moins 30 secondes.

Mode contexte multiple

En mode de contexte multiple, vous ne pouvez partager aucune interface, y compris l'interface de gestion, entre les contextes. Pour assurer la gestion par contexte sur les modèles pris en charge, vous pouvez créer des sous-interfaces de l'interface de gestion et attribuer une sous-interface de gestion à chaque contexte. Certains modèles n'autorisent pas les sous-interfaces sur l'interface de gestion. Par conséquent, la gestion par contexte pour ces modèles nécessite que vous vous connectiez à une interface de données. Pour le Châssis Firepower 4100/9300 , l'interface de gestion et ses sous-interfaces ne sont pas reconnues comme des interfaces de gestion spécialement autorisées dans les contextes; vous devez traiter une sous-interface de gestion comme une interface de données dans ce cas et l'ajouter à une BVI.

Lignes directrices pour la configuration de l'interface de base

Mode de pare-feu transparent

Pour le contexte multiple, en mode transparent, chaque contexte doit utiliser des interfaces différentes; vous ne pouvez pas partager une interface entre contextes.

Basculement

Vous ne pouvez pas partager une interface de basculement ou d'état avec une interface de données.

Directives supplémentaires

Certains services liés à la gestion ne sont pas disponibles jusqu'à ce qu'une interface de non-gestion soit activée et que l'ASA atteigne l'état « Système prêt ». L'ASA génère le message de journal système suivant lorsqu'il est à l'état « Système prêt » :

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

Paramètres par défaut pour la configuration de l'interface de base

Cette section répertorie les paramètres par défaut des interfaces si vous n'avez pas de configuration d'usine par défaut.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface et du mode de contexte.

En mode de contexte multiple, toutes les interfaces allouées sont activées par défaut, quel que soit l'état de l'interface dans l'espace d'exécution du système. Cependant, pour que le trafic passe par l'interface, celle-ci

doit également être activée dans l'espace d'exécution du système. Si vous désactivez une interface dans l'espace d'exécution du système, cette interface est désactivée dans tous les contextes qui la partagent.

En mode unique ou dans l'espace d'exécution du système, les interfaces ont les états par défaut suivants :

- Interfaces physiques : désactivées.
- Sous-interfaces VLAN : activées. Cependant, pour que le trafic passe par la sous-interface, l'interface physique doit également être activée.
- Interfaces VXLAN VNI : activées.
- Interfaces de canal de port EtherChannel (ISA 3000) : activées. Cependant, pour que le trafic passe par l'EtherChannel, les interfaces physiques des groupes de canaux doivent également être activées.
- Interfaces de canal de port EtherChannel (autres modèles) : désactivées.



Remarque Dans le cas du Firepower 4100/9300, vous pouvez activer et désactiver administrativement les interfaces dans le châssis et sur l'ASA. Pour qu'une interface soit opérationnelle, elle doit être activée dans les deux systèmes d'exploitation. Étant donné que l'état de l'interface est contrôlé indépendamment, il se peut que vous ayez une incompatibilité entre le châssis et l'ASA.

Vitesse par défaut et duplex

- Par défaut, la vitesse et les interfaces duplex pour les interfaces en cuivre (RJ-45) sont à négociation automatique.

Type de connecteur par défaut

Certains modèles comprennent deux types de connecteurs : le RJ-45 en cuivre et le SFP à fibre optique. RJ-45 est le type par défaut. Vous pouvez configurer l'ASA pour utiliser les connecteurs SFP à fibre optique.

Adresses MAC par défaut

Par défaut, l'interface physique utilise l'adresse MAC rémanente, et toutes les sous-interfaces d'une interface physique utilisent la même adresse MAC rémanente.

Activer l'interface physique et configurer les paramètres Ethernet

Cette section décrit comment :

- Activer l'interface physique
- Définir une vitesse et un duplex (si disponible)
- (Secure Firewall) Activer les trames de pause pour le contrôle de flux
- (Secure Firewall 3100) Définir la correction d'erreurs sans voie de retour

Avant de commencer

Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Spécifiez l'interface que vous souhaitez configurer :

interface *physical_interface*

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
```

L'ID *physical_interface* comprend le type, le logement et le numéro de port sous la forme type[slot/]port.

Les types d'interfaces physiques sont les suivants :

- **ethernet**

  gigabitethernet
- **tengigabitethernet**
- **management**

Saisissez le type suivi du *logement*/*port*, par exemple, **gigabitEthernet0/1**. Un espace est facultatif entre le type et le logement/port.

Étape 2 (Facultatif) Définissez la vitesse (elle varie en fonction du modèle).

speed {**auto** | *speed* | **nonegotiate** | **sfp-detect**}

Exemple :

```
ciscoasa(config-if)# speed 100
```

Pour les interfaces Firepower 1100 et 2100, le paramètre **speed nonegotiate** définit la vitesse à 1 000 Mbit/s et désactive la négociation de liaison pour les paramètres de contrôle de flux et les renseignements sur les défaillances à distance. Pour le Secure Firewall 3100, consultez la commande **negotiate-auto**.

(Secure Firewall 3100 uniquement) Choisissez **sfp-detect** pour détecter la vitesse du module SFP installé et utiliser la vitesse appropriée. Le mode duplex est toujours complet et la négociation automatique est toujours activée. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement.

Étape 3 (Secure Firewall) Définissez la négociation automatique.

negotiate-auto

La négociation automatique est définie indépendamment de la vitesse.

Exemple :

```
ciscoasa(config-if)# negotiate-auto
```

Étape 4 (Facultatif) Définissez les conditions de duplex pour les interfaces RJ-45 :

duplex {**auto** | **full** | **half**}

Les interfaces SFP prennent uniquement en charge les conditions de duplex intégral.

Exemple :

```
ciscoasa(config-if)# duplex full
```

Étape 5 (Facultatif) (Secure Firewall 3100) Définissez la correction d'erreurs sans voie de retour (FEC) pour les interfaces de 25 Gbit/s et plus.

fec {**auto** | **cl108-rs** | **cl74-fc** | **disable**}

Pour une interface membre d'EtherChannel, vous devez configurer la correction d'erreur directe avant de l'ajouter à l'EtherChannel. Le paramètre choisi lorsque vous utilisez **auto** dépend du type d'émetteur-récepteur et selon si l'interface est fixe (intégrée) ou sur un module de réseau.

Remarque
Si une interface est supprimée de l'EtherChannel, après le redémarrage de votre ASA, la configuration de la FEC et de la négociation automatique sera modifiée. Vous devez configurer manuellement la FEC et la négociation automatique, car il s'agit d'un comportement attendu.

Tableau 24 : FEC par défaut pour le réglage automatique

Type d'émetteur/récepteur	FEC par défaut du port fixe (Ethernet 1/9 à 1/16)	FEC par défaut du module de réseau
25G-SR	cl108-rs	cl108-rs
25G-LR	cl108-rs	cl108-rs
10/25G-CSR	cl108-rs	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	Négociation automatique	Négociation automatique
25G-CU4/5M	Négociation automatique	Négociation automatique

Étape 6 (Facultatif) (Secure Firewall) Activez les trames de pause (XOFF) pour le contrôle de flux sur les interfaces Gigabit et supérieures :

flowcontrol send on

Exemple :

```
ciscoasa(config-if)# flowcontrol send on
```

Le contrôle de flux permet aux ports Ethernet connectés de contrôler les débits de trafic en cas de congestion en permettant aux nœuds encombrés de suspendre les opérations de liaison à l'autre extrémité. Si le port ASA est congestionné (épuisement des ressources en file d'attente sur le commutateur interne) et ne peut plus recevoir de trafic, il en informe l'autre port en envoyant une trame de pause pour interrompre l'envoi jusqu'à

ce que la condition soit réglée. À la réception d'une trame de pause, le périphérique expéditeur arrête d'envoyer des paquets de données, ce qui empêche toute perte de paquets de données pendant la période de congestion.

Remarque
L'ASA prend en charge la transmission de trames de pause afin que l'homologue distant puisse contrôler le débit du trafic.

Cependant, la réception de trames de pause n'est pas prise en charge.

Le commutateur interne dispose d'un ensemble global de 8 000 tampons de 250 octets chacun et le commutateur alloue des tampons de manière dynamique à chaque port. Une trame de pause est envoyée à chaque interface pour laquelle le contrôle de flux est activé lorsque l'utilisation de la mémoire tampon dépasse la borne supérieure globale (2 Mo (8 000 tampons)); et une trame de pause est envoyée par une interface particulière lorsque sa mémoire tampon dépasse le seuil supérieur du port (0,3125 Mo (1 250 tampons)). Après l'envoi d'une pause, une trame XON peut être envoyée lorsque l'utilisation de la mémoire tampon est réduite sous le seuil des faibles niveaux(1,25 Mo dans l'ensemble (5 000 tampons ; 0,25 Mo par port (1 000 tampons)). Le partenaire de liaison peut reprendre le trafic après avoir reçu une trame XON.

Seules les trames de contrôle de flux définies dans la norme 802.3x sont prises en charge. Le contrôle de flux basé sur la priorité n'est pas pris en charge.

Étape 7 Activez l'interface :

no shutdown

Exemple :

```
ciscoasa(config-if)# no shutdown
```

Pour désactiver l'interface, saisissez la commande **shutdown**. Si vous saisissez la commande **shutdown**, vous désactivez également toutes les sous-interfaces. Si vous désactivez une interface dans l'espace d'exécution du système, cette interface est désactivée dans tous les contextes qui la partagent.

Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000)

Une trame étendue est un paquet Ethernet supérieur au maximum standard de 1518 octets (y compris l'en-tête de couche 2 et l'en-tête VLAN) qui peut s'élever jusqu'à 9216 octets. Vous pouvez activer la prise en charge des trames étendues pour toutes les interfaces en augmentant la quantité de mémoire nécessaire pour traiter les trames Ethernet. L'attribution de plus de mémoire aux trames étendues peut limiter l'utilisation maximale d'autres fonctionnalités, telles que les listes de contrôle d'accès. Remarque : la MTU ASA définit la taille de la charge utile sans inclure la couche 2 (14 octets) et l'en-tête VLAN (4 octets), donc la MTU maximale peut s'élever à 9198, selon votre modèle.

Cette procédure s'applique uniquementà l'ISA 3000, et à l'ASA virtuel. D'autres modèles prennent en charge les bâtis grand format par défaut.

Les bâtis grand format ne sont pas pris en charge sur les ASAv5 et ASAv10 avec moins de 8 Go de RAM.

Avant de commencer

- En mode contexte multiple, définissez cette option dans l'espace d'exécution du système.
- Les modifications de ce paramètre nécessitent que vous rechargiez l'ASA.
- Assurez-vous de définir la MTU pour chaque interface devant transmettre des trames étendues à une valeur supérieure à la valeur par défaut 1500; par exemple, définissez la valeur sur 9198 à l'aide de la commande **mtu** . En mode contexte multiple, définissez la MTU dans chaque contexte.
- Veillez à régler le TCP MSS, soit pour le désactiver pour le trafic non-IPsec (utilisez la commande **sysopt connection tcpmss 0**), soit pour l'augmenter en fonction de la MTU.

Procédure

Activer la prise en charge des trames étendues

jumbo-frame reservation

Exemples

L'exemple suivant active la réservation des trames étendues, enregistre la configuration et recharge l'ASA :

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

Gérer le module de réseau pour Cisco Secure Firewall

Si vous installez un module de réseau avant de mettre le pare-feu sous tension pour la première fois, aucune action n'est requise; le module de réseau est activé et prêt à l'emploi.

Si vous devez apporter des modifications à l'installation de votre module de réseau après le démarrage initial, consultez les procédures suivantes.

Configurer les ports d'éclatement

Vous pouvez configurer des ports d'épanouissement de 10 Go pour chaque interface de 40 Go ou plus. Cette procédure vous explique comment rompre et rejoindre les ports. Les ports d'épanouissement peuvent être utilisés comme n'importe quel autre port Ethernet physique, y compris lorsqu'ils sont ajoutés aux EtherChannels.

Si une interface est déjà utilisée dans votre configuration, vous devrez supprimer manuellement toute configuration liée aux interfaces qui ne seront plus présentes.

Avant de commencer

- Vous devez utiliser un câble épanoui pris en charge. Consultez le guide d'installation du matériel pour plus d'informations.
- Pour la mise en grappe ou le basculement, assurez-vous que la liaison de basculement n'utilise pas l'interface parent (pour la séparation) ou l'interface enfant (pour la jonction); vous ne pouvez pas apporter de modifications à l'interface si elle est utilisée pour la liaison de grappe/basculement.

Procédure

Étape 1 Séparez les ports de 10 Go d'une interface de 40 Go ou plus.

breakout *slot port*

Par exemple, pour diviser l'interface Ethernet2/1 de 40 Go, vous devez spécifier **2** pour le *logement* et **1** pour le *port*. Les interfaces enfants résultantes seront identifiées comme Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3 et Ethernet2/1/4.

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; les modifications d'interface sont répliquées sur les autres nœuds.

Exemple :

```
ciscoasa(config)# breakout 2 1
ciscoasa(config)# breakout 2 2
ciscoasa(config)# breakout 2 3
ciscoasa(config)# breakout 2 4
```

Étape 2 Rejoignez les ports d'éclatement pour restaurer l'interface.

no breakout *slot port*

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Vous devez joindre tous les ports enfants de l'interface.

Exemple :

```
ciscoasa(config)# no breakout 2 1
```

Ajouter un module de réseau

Pour ajouter un module de réseau à un pare-feu après le démarrage initial, procédez comme suit. L'ajout d'un nouveau module nécessite un rechargement. Pour la mise en grappe ou le basculement, aucun temps d'arrêt n'est pris en charge. Veuillez donc vous assurer d'effectuer cette procédure pendant une fenêtre de maintenance.

Procédure

Étape 1 Installez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez installer le module de réseau lorsque le pare-feu est sous tension.

Pour la mise en grappe ou le basculement, installez le module de réseau sur tous les nœuds.

Étape 2 Rechargez le pare-feu; consultez Recharger l'ASA, à la page 45.

Pour la mise en grappe ou le basculement, rechargez tous les nœuds. Étant donné que les nœuds dotés de modules de réseau différents ne peuvent pas rejoindre la paire de grappe/basculement, vous devez recharger tous les nœuds avec le nouveau module avant qu'ils puissent reformer la paire de grappe/basculement.

Étape 3 Activez le module de réseau.

no netmod 2 disable

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Exemple :

```
ciscoasa(config)# no netmod 2 disable
```

Échange à chaud du module de réseau

Vous pouvez échanger à chaud un module de réseau contre un nouveau module du même type sans avoir à recharger. Cependant, vous devez arrêter le module actuel pour le retirer en toute sécurité. Cette procédure décrit comment arrêter l'ancien module, installer un nouveau module et l'activer.

Pour la mise en grappe ou le basculement, vous ne pouvez pas désactiver un module de réseau si la liaison de commande de grappe ou de basculement se trouve sur le module.

Procédure

Étape 1 Pour la mise en grappe ou le basculement, procédez comme suit :

- **Mise en grappe** : assurez-vous que l'unité sur laquelle vous souhaitez effectuer l'échange à chaud est un nœud de données (voir Modifier le nœud de contrôle, à la page 401); puis désactivez la mise en grappe sur le nœud. Reportez-vous aux sections Devenir un nœud inactif, à la page 398 ou Désactiver undonnées, à la page 399.

Si la liaison de commande de grappe se trouve sur le module de réseau, vous devez quitter la grappe. Consultez Quitter la grappe, à la page 400. La désactivation du module de réseau avec une liaison de commande de grappe active n'est pas autorisée.

- **Basculement** : assurez-vous que l'unité sur laquelle vous souhaitez effectuer l'échange à chaud est le nœud de secours. Consultez Forcer le basculement, à la page 319.

  Si la liaison de basculement se trouve sur le module de réseau, vous devez désactiver le basculement. Consultez Désactiver le basculement, à la page 320. La désactivation du module de réseau avec un lien de basculement actif n'est pas autorisée.

Étape 2 Désactivez le module de réseau.

netmod 2 disable

Exemple :

```
ciscoasa(config)# netmod 2 disable
```

Étape 3 Remplacez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez remplacer le module de réseau lorsque le pare-feu est sous tension.

Étape 4 Activez le module de réseau.

no netmod 2 disable

Exemple :

```
ciscoasa(config)# no netmod 2 disable
```

Étape 5 Pour la mise en grappe ou le basculement, procédez comme suit :

- Mise en grappe : **rajoutez** le nœud à la grappe. Consultez Rejoindre la grappe, à la page 399.
- **Basculement** : si vous avez désactivé le basculement, veuillez le reconfigurer.

Remplacer le module de réseau par un module de type différent

Si vous remplacez un module de réseau par un autre type, un rechargement est nécessaire. Si le nouveau module comporte moins d'interfaces que l'ancien module, vous devrez supprimer manuellement toute configuration liée aux interfaces qui ne seront plus présentes. Pour la mise en grappe ou le basculement, aucun temps d'arrêt n'est pris en charge. Veuillez donc vous assurer d'effectuer cette procédure pendant une fenêtre de maintenance.

Procédure

Étape 1 Désactivez le module de réseau.

netmod 2 disable

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds. N'enregistrez pas la configuration; lors du rechargement, le module sera activé à l'aide de la configuration enregistrée.

Exemple :

```
ciscoasa(config)# netmod 2 disable
```

Étape 2 Remplacez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez remplacer le module de réseau lorsque le pare-feu est sous tension.

Pour la mise en grappe ou le basculement, installez le module de réseau sur tous les nœuds.

Étape 3 Rechargez le pare-feu; consultez Recharger l'ASA, à la page 45.

Pour la mise en grappe ou le basculement, rechargez tous les nœuds. Étant donné que les nœuds dotés de modules de réseau différents ne peuvent pas rejoindre la paire de grappe/basculement, vous devez recharger tous les nœuds avec le nouveau module avant qu'ils puissent reformer la paire de grappe/basculement.

Étape 4 Si vous avez enregistré la configuration avant le rechargement, vous devrez réactiver le module.

Retirer le module de réseau

Si vous souhaitez retirer définitivement le module de réseau, procédez comme suit. Le retrait d'un module de réseau nécessite un rechargement. Pour la mise en grappe ou le basculement, aucun temps d'arrêt n'est pris en charge. Veuillez donc vous assurer d'effectuer cette procédure pendant une fenêtre de maintenance.

Avant de commencer

Pour la mise en grappe ou le basculement, assurez-vous que la liaison de basculement ne se trouve pas sur le module de réseau; dans ce cas, vous ne pouvez pas retirer le module.

Procédure

Étape 1 Désactivez le module de réseau et enregistrez la configuration.

netmod 2 disable

write memory

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Exemple :

```
ciscoasa(config)# netmod 2 disable
ciscoasa(config)# write memory
```

Étape 2 Retirez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez retirer le module de réseau lorsque le pare-feu est sous tension.

Pour la mise en grappe ou le basculement, retirez le module de réseau sur tous les nœuds.

Étape 3 Rechargez le pare-feu; consultez Recharger l'ASA, à la page 45.

Pour la mise en grappe ou le basculement, rechargez tous les nœuds. Étant donné que les nœuds dotés de modules de réseau différents ne peuvent pas rejoindre la paire de grappe/basculement, vous devez recharger tous les nœuds sans le module avant qu'ils puissent reformer la paire de grappe/basculement.

Surveillance des interfaces

Consultez les commandes suivantes.

Remarque Pour les modèles Firepower et Secure Firewall, certaines statistiques ne sont pas affichées à l'aide des commandes ASA. Vous devez consulter des statistiques d'interface plus détaillées à l'aide des commandes FXOS.

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

Pour Firepower 2100 en mode plateforme, consultez aussi les commandes FXOS connect local-mgmt suivantes :

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

Consultez le guide de dépannage FXOS pour plus d'informations.

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

Exemples d'interfaces de base

Consultez les exemples de configuration suivants.

Exemple de paramètres d'interface physique

L'exemple suivant configure les paramètres de l'interface physique en mode unique :

```
interface gigabitethernet 0/1
speed 1000
```

```
duplex full
no shutdown
```

Exemple de mode de contexte multiple

L'exemple suivant configure les paramètres d'interface en mode de contexte multiple pour la configuration système et attribue la sous-interface gigabitEthernet 0/1.1 à contexteA :

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

Historique de la configuration de l'interface de base

Tableau 25 : Historique des interfaces

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
La correction d'erreur par défaut (FEC) sur les ports fixes du Secure Firewall 3100 est passée de cl74-fc à cl108-rs pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+.	9.18(3)/9.19(1)	Lorsque vous définissez le FEC sur Auto sur les ports fixes du Secure Firewall 3100, le type par défaut est désormais défini sur cl108-rs au lieu de cl74-fc pour les émetteurs-récepteurs SR, CSR et LR de 25 Go. Commandes nouvelles/modifiées : **fec**
Mettre en pause les trames pour le contrôle de flux sur Cisco Secure Firewall 3100	9.18(1)	S'il y a une rafale de trafic, des paquets abandonnés peuvent se produire si la rafale dépasse la capacité de mise en mémoire tampon de la mémoire tampon FIFO sur la carte réseau et les mémoires tampons des anneaux de réception. L'activation des trames de pause pour le contrôle de flux peut atténuer ce problème. Commandes nouvelles ou modifiées : **flowcontrol send on**
Ports d'éclatement pour Secure Firewall 3130 et 3140	9.18(1)	Vous pouvez maintenant configurer quatre ports d'éclatement de 10 Go pour chaque interface de 40 Go sur les Cisco Secure Firewall 3130 et 3140. Commandes nouvelles ou modifiées : **breakout**
Prise en charge de l'échange à chaud du module de réseau pour Secure Firewall 3100	9.17(1)	Vous pouvez ajouter ou retirer le module de réseau sur le pare-feu Secure Firewall 3100 lorsque le pare-feu est sous tension. Pour remplacer un module par un autre module du même type, vous n'avez pas besoin de redémarrer. Après le démarrage initial, l'ajout d'un module, le retrait permanent d'un module ou le remplacement d'un module par un nouveau type nécessite un redémarrage. Commandes nouvelles ou modifiées : **netmod**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de la correction d'erreurs sans voie de retour pour Cisco Secure Firewall 3100	9.17(1)	Les interfaces de Cisco Secure Firewall 3100 25 Gbit/s prennent en charge la correction d'erreurs sans voie de retour (FEC). La FEC est activée par défaut et définie sur Auto. Commandes nouvelles ou modifiées : **fec**
Prise en charge du réglage de la vitesse en fonction du SFP pour Secure Firewall 3100	9.17(1)	Le pare-feu Secure Firewall 3100 prend en charge la détection de la vitesse pour les interfaces basées sur SFP installées. La détection de SFP est activée par défaut. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement. Commandes nouvelles ou modifiées : **speed sfp-detect**
La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée pour les interfaces de 1 Gigabit et les versions ultérieures.	9.17(1)	La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée séparément de la vitesse pour les interfaces de 1 Gigabit et les versions ultérieures. Commandes nouvelles ou modifiées : **negotiate-auto**
La négociation automatique de la vitesse peut être désactivée sur les interfaces à fibre optique sur les périphériques Firepower 1100 et 2100.	9.14(1)	Vous pouvez maintenant configurer une interface à fibre optique Firepower 1100 ou 2100 pour désactiver la négociation automatique. Pour les interfaces de 10 Go, vous pouvez configurer la vitesse à 1 Go sans négociation automatique; vous ne pouvez pas désactiver la négociation automatique pour une interface dont la vitesse est réglée à 10 Go. Commandes nouvelles ou modifiées : **speed nonegotiate**
Prise en charge du trafic de transit sur l'interface de gestion Management 0/0 pour l'ASA virtuel	9.6(2)	Vous pouvez maintenant autoriser le trafic de transit sur l'interface de gestion Management 0/0 sur l'ASA virtuel. Auparavant, seul l'ASA virtuel sur Microsoft Azure prenait en charge le trafic de transit; maintenant, tous les ASA virtuel le prennent en charge. Vous pouvez éventuellement configurer cette interface pour qu'elle soit en gestion uniquement, mais elle n'est pas configurée par défaut. Nous avons modifié la commande suivante : **management-only**
Prise en charge des trames de pause pour le contrôle de flux sur les interfaces Gigabit Ethernet	8.2(5)/8.4(2)	Vous pouvez maintenant activer des trames de pause (XOFF) pour le contrôle de flux des interfaces Gigabit Ethernet sur tous les modèles ASA. Nous avons modifié la commande suivante : **flowcontrol**.
Prise en charge des trames de pause pour le contrôle de flux sur les interfaces ASA 5580 10 Gigabit Ethernet	8.2(2)	Vous pouvez maintenant activer des trames de pause (XOFF) pour le contrôle de flux. Cette fonctionnalité est également prise en charge sur l'ASA 5585-X. Nous avons introduit la commande suivante : **flowcontrol**.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge des paquets étendus pour l'ASA 5580	8.1(1)	L'ASA 5580 prend en charge les bâtis grand format. Une trame étendue est un paquet Ethernet supérieur au maximum standard de 1 518 octets (y compris l'en-tête de couche 2 et FCS) qui peut s'élever jusqu'à 9 216 octets. Vous pouvez activer la prise en charge des trames étendues pour toutes les interfaces en augmentant la quantité de mémoire nécessaire pour traiter les trames Ethernet. L'attribution de plus de mémoire aux trames étendues peut limiter l'utilisation maximale d'autres fonctionnalités, telles que les listes de contrôle d'accès. Cette fonctionnalité est également prise en charge sur l'ASA 5585-X. Nous avons introduit la commande suivante : **jumbo-frame reservation**.
Prise en charge de Gigabit Ethernet pour la licence Security Plus sur l'ASA 5510	7.2(3)	L'ASA 5510 prend désormais en charge GE (Gigabit Ethernet) pour les ports 0 et 1 avec la licence Security Plus. Si vous mettez à niveau la licence de base vers Security Plus, la capacité des ports Ethernet0/0 et Ethernet0/1 externes passe de FE (Fast Ethernet) (100 Mbps) à GE (1 000 Mbps). Les noms d'interface resteront Ethernet 0/0 et Ethernet 0/1. Utilisez la commande **speed** pour modifier la vitesse sur l'interface et utilisez la commande **show interface** pour voir quelle vitesse est actuellement configurée pour chaque interface.
Augmentation du nombre d'interfaces pour la licence de base sur l'ASA 5510	7.2(2)	Pour la licence de base sur l'ASA 5510, le nombre maximum d'interfaces est passé de 3 plus une interface de gestion à un nombre illimité d'interfaces.



CHAPITRE 15

Configuration de base de l'interface pour les ports de commutation du Firepower 1010

Vous pouvez configurer chaque interface Firepower 1010 pour qu'elle fonctionne comme une interface pare-feu normale ou comme un port de commutateur matériel de couche 2. Ce chapitre comprend les tâches de démarrage de la configuration de votre port de commutation, notamment l'activation ou la désactivation du mode de commutation, la création d'interfaces VLAN et l'affectation des ports de commutation aux réseaux VLAN. Ce chapitre décrit également comment personnaliser l'alimentation par Ethernet (PoE) sur les interfaces prises en charge.

- À propos des ports de commutation, à la page 689
- Lignes directrices et limites pour les ports de commutation, à la page 690
- Configurer les ports de commutation et l'alimentation par Ethernet (PoE), à la page 692
- Supervision des ports de commutation, à la page 700
- Exemples de ports de commutation, à la page 701
- Historique des ports de commutation, à la page 705

À propos des ports de commutation

Cette section décrit les ports de commutation du Firepower 1010 et du .

Comprendre les ports et les interfaces de commutation

Ports et interfaces

Pour chaque interface physique 1010, vous pouvez définir son fonctionnement comme interface de pare-feu ou comme port de commutation. Consultez les renseignements suivants sur les interfaces physiques et les types de port, ainsi que sur les interfaces VLAN logiques auxquelles vous affectez des ports de commutation :

- Interface de pare-feu physique : En mode routé, ces interfaces transmettent le trafic entre les réseaux de la couche 3 en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu et VPN. En mode transparent, ces interfaces sont des membres de groupes de ponts qui acheminent le trafic entre les interfaces du même réseau au niveau de la couche 2, en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu. En mode routé, vous pouvez également utiliser le routage et le pont intégrés avec certaines interfaces comme membres du groupe de ponts et d'autres comme interfaces de couche 3. Par défaut, l'interface Ethernet 1/1 est configurée comme interface de pare-feu.

- Port de commutation physique : les ports de commutation transfèrent le trafic à la couche 2 en utilisant la fonction de commutation dans le matériel. Les ports de commutation sur le même VLAN peuvent communiquer entre eux grâce à la commutation matérielle, et le trafic n'est pas soumis à la politique de sécurité ASA. Les ports d'accès acceptent uniquement le trafic non balisé et vous pouvez les affecter à un seul VLAN. Les ports de ligne principale acceptent le trafic non balisé et peuvent appartenir à plus d'un VLAN. Par défaut, Ethernet 1/2 à 1/8 sont configurés comme ports de commutation d'accès sur VLAN 1. Vous ne pouvez pas configurer l'interface Management (gestion) comme port de commutation.
- Logical VLAN interface (interface VLAN logique) : Ces interfaces fonctionnent de la même façon que les interfaces de pare-feu physiques, à la différence que vous ne pouvez pas créer des sous-interfaces, des , des ou des interfaces EtherChannel. Lorsqu'un port de commutation doit communiquer avec un autre réseau, le périphérique ASA applique la politique de sécurité à l'interface VLAN et achemine le routage vers une autre interface VLAN logique ou une interface de pare-feu. Vous pouvez même utiliser le routage et le pont intégrés avec des interfaces VLAN comme membres du groupe de ponts. Le trafic entre les ports de commutation sur le même VLAN n'est pas soumis à la politique de sécurité, mais le trafic entre les VLAN d'un groupe de ponts est soumis à la politique de sécurité ASA. Vous pouvez donc choisir de superposer les groupes de ponts et les ports de commutation pour appliquer la politique de sécurité entre certains segments.

Alimentation par Ethernet

La PoE est disponible sur Ethernet 1/7 et Ethernet 1/8 en utilisant les protocoles IEEE 802.3af (PoE) et 802.3at (PoE+), jusqu'à 30 W par port.

PoE+ utilise le protocole LLDP (Link Layer Discovery Protocol) pour négocier le niveau de puissance. L'alimentation n'est fournie qu'en cas de besoin.

Si vous désactivez l'interface, vous désactivez l'alimentation du périphérique.

Fonctionnalité Auto-MDI/MDIX

Pour tous les ports de commutation, le paramètre de négociation automatique par défaut inclut également la fonction Auto-MDI/MDIX. La fonction Auto-MDI/MDIX élimine le besoin de câblage croisé en effectuant un croisé interne lorsqu'un câble droit est détecté pendant la phase de négociation automatique. La vitesse ou le duplex doivent être réglés pour qu'ils soient négociés automatiquement afin d'activer Auto-MDI/MDIX pour l'interface. Si vous définissez explicitement la vitesse et le duplex à une valeur fixe, désactivant ainsi la négociation automatique pour les deux paramètres, Auto-MDI/MDIX est également désactivé. Lorsque la vitesse et le mode duplex sont définis à 1000 et que la vitesse maximale est atteinte, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

Lignes directrices et limites pour les ports de commutation

Mode contextuel

- Firepower 1010 ne prend pas en charge le mode contexte multiple.
- Le Secure Firewall 1210/1220 ne prend pas en charge le mode de contexte multiple.

Failover (basculement) et mise en grappe

- Aucune prise en charge de grappe.
- Prise en charge du basculement actif/veille uniquement.
- Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de Failover (basculement). Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. Failover (basculement) est conçu pour empêcher le trafic de passer par l'unité en veille, mais cette fonctionnalité ne s'étend pas aux ports de commutation. Dans une configuration réseau Failover (basculement) normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d'utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser Failover (basculement) avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
- Vous ne pouvez utiliser qu'une interface de pare-feu comme liaison de basculement.

Interfaces logiques VLAN (SVI)

- Vous pouvez créer jusqu'à 60 interfaces VLAN.
- Si vous utilisez également des sous-interfaces VLAN sur une interface de pare-feu, vous ne pouvez pas utiliser le même ID VLAN que pour une interface VLAN logique.
- Adresses MAC
  - Mode de pare-feu routé : toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez Configurer manuellement l'adresse MAC, à la page 807
  - Mode pare-feu transparent : chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez Configurer manuellement l'adresse MAC, à la page 807.

Groupes de ponts

Vous ne pouvez pas mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques dans le même groupe de ponts.

Fonctionnalités non prises en charge de l'interface VLAN et du port de commutation

Les interfaces VLAN et les ports de commutation ne prennent pas en charge :

- Routage dynamique
- Routage multidiffusion
- Routage basé sur les politiques
- Routage multiples chemins à coûts égaux (ECMP)
- VXLAN

- EtherChannels : les ports de commutation ne peuvent pas faire partie d'un EtherChannel. Le PoE n'est pas non plus pris en charge sur un port d'un EtherChannel.
- Basculement et lien d'état
- Zones de circulation
- Balise du groupe de sécurité (SGT)

Autres directives et limites

- Vous pouvez configurer un maximum de 60 interfaces nommées sur le Firepower 1010.
- Vous ne pouvez pas configurer l'interface Management (gestion) comme port de commutation.

Paramètres d'usine

- Ethernet 1/1 est une interface de pare-feu.
- Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.
- Vitesse et duplex par défaut: par défaut, la vitesse et le duplex sont configurés pour la négociation automatique.

Configurer les ports de commutation et l'alimentation par Ethernet (PoE)

Pour configurer les ports de commutation et la PoE, procédez comme suit :

Activer ou désactiver le mode Port de commutation

Vous pouvez définir chaque interface indépendamment comme interface de pare-feu ou comme port de commutation. Par défaut, Ethernet 1/1 est une interface de pare-feu et les autres interfaces Ethernet sont configurées comme des ports de commutation.

Procédure

Étape 1 Entrez en mode de configuration d'interface.

interface ethernet1/*port*

- *port* : définit le port, de 1 à 8.

Vous ne pouvez pas définir l'interface de gestion Management 1/1 sur le mode du port de commutation.

Exemple :

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

Étape 2 Activez le mode Port de commutation.

switchport

Si cette interface est déjà en mode Port de commutation, vous êtes invité à configurer les paramètres du port de commutation au lieu de modifier le mode.

```
ciscoasa(config-if)# switchport
ciscoasa(config-if)# switchport ?
interface mode commands/options:
  access         Set access mode characteristics of the interface
  mode           Set trunking mode of the interface
  monitor        Monitor another interface
  protected      Configure an interface to be a protected port
  trunk          Set trunking characteristics of the interface
<cr>
ciscoasa(config-if)#
```

Étape 3 Désactivez le mode Port de commutation.

no switchport

```
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# switchport ?

interface mode commands/options:
<cr>
```

Exemple

L'exemple suivant définit Ethernet 1/3 et 1/4 en mode de pare-feu :

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)#
```

Configurer une interface VLAN

Cette section décrit comment configurer les interfaces VLAN (SVI) à utiliser avec les ports de commutation associés. Vous pouvez créer jusqu'à 60 interfaces VLAN associées aux ports de commutation.

Procédure

Étape 1 Ajoutez une interface VLAN.

interface vlan *ID*

- *id* : définit l'ID de VLAN pour cette interface, entre 1 et 4070, en excluant les ID de 3968 à 4047, qui sont réservés à un usage interne.

Exemple :

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)#
```

Étape 2 (Facultatif) Désactivez le transfert vers un autre VLAN.

no forward interface *vlan_id*

- *vlan_id* : spécifie l'ID de VLAN vers lequel cette interface VLAN ne peut pas initier le trafic.

Par exemple, vous avez un VLAN affecté à l'extérieur pour l'accès Internet, un VLAN affecté à un réseau interne d'entreprise et un troisième VLAN affecté à votre réseau domestique. Le réseau domestique n'a pas besoin d'accéder au réseau de l'entreprise, vous pouvez donc utiliser la commande **no forward interface** sur le VLAN domestique; le réseau professionnel peut accéder au réseau domestique, mais le réseau domestique ne peut pas accéder au réseau d'entreprise.

Exemple :

```
ciscoasa(config-if)# no forward interface 200
ciscoasa(config-if)#
```

Configurer les ports de commutation comme ports d'accès

Pour affecter un port de commutation à un seul VLAN, configurez-le comme port d'accès. Les ports d'accès acceptent uniquement le trafic non balisé. Par défaut, Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.



Remarque L'appareil ne prend pas en charge le protocole Spanning Tree pour la détection de boucle dans le réseau. Par conséquent, vous devez vous assurer qu'une connexion avec l'ASA ne finit pas dans une boucle de réseau.

Procédure

Étape 1 Entrez en mode de configuration d'interface.

interface ethernet1/*port*

- *port* : définit le port, de 1 à 8.

Exemple :

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

Étape 2 Attribuez ce port de commutation à un VLAN.

switchport access vlan *number*

- *number* : définit l'ID de VLAN entre 1 et 4070. La valeur par défaut est VLAN 1.

Exemple :

```
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)#
```

Étape 3 (Facultatif) Définissez ce port de commutation comme protégé afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

switchport protected

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres si vous appliquez la commande **switchport protected** à chaque port de commutation. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Exemple :

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

Étape 4 (Facultatif) Définissez la vitesse.

speed {**auto** | **10** | **100** | **1000**}

La valeur par défaut est **auto**.

Exemple :

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

Étape 5 (Facultatif) Définissez le duplex.

duplex {**auto** | **full** | **half**}

La valeur par défaut est **auto**.

Exemple :

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

Étape 6 Activez le port de commutation.

no shutdown

Pour désactiver le port de commutation, saisissez la commande **shutdown**.

Exemple :

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

Exemple

L'exemple suivant affecte Ethernet 1/3, Ethernet 1/4 et Ethernet 1/5 au VLAN 101 et définit Ethernet 1/3 et Ethernet 1/4 comme protégés :

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/4
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/5
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# no shutdown
```

Configurer les ports de commutation comme ports de ligne principale

Cette procédure décrit comment créer un port de liaison qui peut acheminer plusieurs VLAN à l'aide du balisage 802.1Q. Les ports de ligne principale acceptent le trafic non balisé et balisé. Le trafic sur les VLAN autorisés passe par le port de liaison sans changement.

Lorsque la ligne principale reçoit un trafic non balisé, elle le balise à l'ID de VLAN natif afin que l'ASA puisse transférer le trafic vers les ports de commutation appropriés ou l'acheminer vers une autre interface de pare-feu. Lorsque l'ASA envoie le trafic d'ID de VLAN natif hors du port de liaison, il supprime la balise VLAN. Assurez-vous de définir le même VLAN natif sur le port de liaison de l'autre commutateur afin que le trafic non balisé soit balisé vers le même VLAN.

Procédure

Étape 1 Entrez en mode de configuration d'interface.

interface ethernet1/*port*

- *port* : définit le port, de 1 à 8.

Exemple :

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

Étape 2 Configurez ce port de commutateur en tant que port de liaison.

switchport mode trunk

Pour rétablir ce port en mode d'accès, saisissez la commande **switchport mode access**.

Exemple :

```
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)#
```

Étape 3 Attribuez des VLAN à cette liaison.

switchport trunk allowed vlan *vlan_range*

- *vlan_range* : définit les ID de VLAN entre 1 et 4070. Vous pouvez identifier jusqu'à 20 identifiants de l'une des manières suivantes :
  - Nombre unique (n)
  - Plage A (n à x)
  - Chiffres et plages séparés par des virgules, par exemple :

    5,7-10,13,45-100

  Vous pouvez saisir des espaces au lieu de virgules, mais la commande est enregistrée dans la configuration avec des virgules.

  Si vous incluez le VLAN natif dans cette commande, il est ignoré; le port de liaison supprime toujours le balisage VLAN lors de l'envoi de trafic VLAN natif hors du port. De plus, il ne recevra pas le trafic qui a toujours un balisage VLAN natif.

Exemple :

```
ciscoasa(config-if)# switchport trunk allowed vlan 100,200,300
ciscoasa(config-if)#
```

Étape 4 Définissez le VLAN natif.

switchport trunk native vlan *vlan_id*

- *vlan_range* : définit l'ID de VLAN entre 1 et 4070. La valeur par défaut est VLAN 1.

Chaque port ne peut avoir qu'un seul VLAN natif, mais chaque port peut avoir le même VLAN natif ou un différent.

Exemple :

```
ciscoasa(config-if)# switchport trunk native vlan 2
ciscoasa(config-if)#
```

Étape 5 (Facultatif) Définissez ce port de commutation comme protégé afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

switchport protected

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous

n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres si vous appliquez la commande **switchport protected** à chaque port de commutation. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Exemple :

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

Étape 6 (Facultatif) Définissez la vitesse.

speed {**auto** | **10** | **100** | **1000**}

La valeur par défaut est **auto**.

Exemple :

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

Étape 7 (Facultatif) Définissez le duplex.

duplex {**auto** | **full** | **half**}

La valeur par défaut est **auto**.

Exemple :

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

Étape 8 Activez le port de commutation.

no shutdown

Pour désactiver le port de commutation, saisissez la commande **shutdown**.

Exemple :

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

Exemple

L'exemple suivant définit Ethernet 1/6 comme port de liaison avec les VLAN 20 à 30 et définit le VLAN natif comme 4 :

```
ciscoasa(config)# interface ethernet1/6
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 20-30
ciscoasa(config-if)# switchport trunk native vlan 4
```

```
ciscoasa(config-if)# no shutdown
```

Configurer Power Over Ethernet (alimentation électrique par câble Ethernet)

Les ports Power over Ethernet (PoE) alimentent les périphériques tels que les téléphones IP ou les points d'accès sans fil. Le mode PoE est activé par défaut. Cette procédure décrit comment activer et désactiver la PoE et comment définir les paramètres facultatifs.

Procédure

Étape 1 Entrez en mode de configuration d'interface.

interface ethernet1/{**7** | **8**}

Exemple :

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)#
```

Étape 2 Activez ou désactivez PoE.

power inline {**auto** | **never** | **consumption wattage** *milliwatts*}

- **auto** : fournit automatiquement du courant au périphérique alimenté en utilisant une puissance appropriée pour la classe du périphérique alimenté. Le pare-feu utilise LLDP pour négocier davantage la puissance en watts. Lorsque vous connectez un périphérique d'une certaine classe, il sera provisionné au maximum pour cette classe au cas où il aurait besoin d'utiliser plus de puissance. Par exemple, si vous ajoutez un périphérique de classe 4 qui demande 12,95 W, il se verra attribuer 30 W même s'il n'utilise pas actuellement toute cette puissance. Certains appareils peuvent renégocier les besoins en matière d'alimentation. Si vous savez que votre périphérique a besoin de moins d'alimentation que ce qui est alloué, vous pouvez plutôt définir la **consumption wattage** manuellement pour libérer de l'alimentation pour d'autres périphériques.
- **never** : désactive le PoE.
- **consumption wattage** *milliwatts* : spécifie manuellement la puissance en milliwatts, de 4 000 à 30 000. Utilisez cette commande si vous souhaitez définir les watts manuellement et désactiver la négociation LLDP. Pour l'attribution manuelle, la classe s'affichera comme **n/a** (s.o.) dans la sortie d'affichage, car la classe n'est pas utilisée pour déterminer la consommation d'énergie.

Affichez l'état PoE actuel à l'aide de la commande **show power inline**.

Exemple :

```
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
```

```
Ethernet1/5   n/a     n/a     n/a            n/a
Ethernet1/6   n/a     n/a     n/a            n/a
Ethernet1/7   On      4       121.00         53.00
Ethernet1/8   On      4       88.00          53.00
```

Exemple

L'exemple suivant définit manuellement la puissance en watts pour Ethernet 1/7 et règle la puissance à « auto » pour Ethernet 1/8 :

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

Supervision des ports de commutation

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

- **show switch vlan**

  Affiche l'association du port VLAN au commutateur.

```
ciscoasa# show switch vlan
VLAN Name                    Status    Ports
---- --------------------- --------- --------------------
1    -                      down      Ethernet1/3,
                                      Ethernet1/4,
                                      Ethernet1/5,
                                      Ethernet1/6
                                      Ethernet1/7,
                                      Ethernet1/8
10   inside                 up        Ethernet1/1
20   outside                up        Ethernet1/2
```

- **show switch mac-address-table**

  Affiche les entrées d'adresse MAC statiques et dynamiques.

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds
  Mac Address  | VLAN |       Type       | Age | Port
-----------------------------------------------------
0c75.bd11.c504 | 0010 |     dynamic      | 330 | In0/0
885a.92f6.c6e3 | 0010 |     dynamic      | 330 | Et1/1
0c75.bd11.c504 | 0020 |     dynamic      | 330 | In0/0
```

```
885a.92f6.c45b | 0020 |     dynamic      | 330 | Et1/2
```

- **show arp**

  Affiche les entrées ARP dynamiques, statiques et de mandataire. Les entrées ARP dynamiques comprennent l'ancienneté de l'entrée ARP en secondes. Les entrées ARP statiques comprennent un tiret (-) au lieu de l'âge, et les entrées ARP du mandataire indiquent « alias ». Voici un exemple de sortie de la commande **show arp**. La première entrée est une entrée dynamique de 2 secondes. La deuxième entrée est une entrée statique et la troisième entrée provient d'un mandataire ARP.

```
ciscoasa# show arp
outside 10.86.194.61 0011.2094.1d2b 2
outside 10.86.194.1 001a.300c.8000 -
outside 10.86.195.2 00d0.02a8.440a alias
```

- **show power inline**

  Affichez l'état PoE+.

```
ciscoasa# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

Exemples de ports de commutation

Les rubriques suivantes fournissent des exemples de configuration des ports de commutation en mode routé et transparent.

Exemple de mode routé

L'exemple suivant crée deux interfaces VLAN et affecte deux ports de commutation à l'interface interne et un à l'interface externe.

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0
no shutdown
!
```

```
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

Exemple de mode transparent

L'exemple suivant crée deux interfaces VLAN dans le groupe de ponts 1 et affecte deux ports de commutation à l'interface interne et un à l'interface externe.

```
firewall transparent
!
interface BVI1
ip address 10.20.20.1 255.255.255.0
!
interface Vlan11
bridge-group 1
nameif inside
security-level 100
no shutdown
!
interface Vlan20
bridge-group 1
nameif outside
security-level 0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

Exemple d'interface de pare-feu/port de commutation mixte

L'exemple suivant crée une interface VLAN pour l'interface interne et deux interfaces de pare-feu pour l'interface externe et DMZ.

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/4
nameif outside
security-level 0
ip address 10.12.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/5
nameif dmz
security-level 50
ip address 10.13.11.1 255.255.255.0
no shutdown
```

Exemple de routage et pont intégrés

L'exemple suivant crée deux groupes de ponts, avec deux interfaces VLAN (interne_1 et interne_2) dans le groupe de ponts 1 et une (externe) dans le groupe de ponts 2. Une quatrième interface VLAN ne fait pas partie d'un groupe de ponts et constitue une interface routée standard. Le trafic entre les ports de commutation sur le même VLAN n'est pas soumis à la politique de sécurité de l'ASA. Toutefois, le trafic entre les VLAN d'un groupe de ponts est soumis à la politique de sécurité. Vous pouvez donc choisir de superposer les groupes de ponts et les ports de commutation pour appliquer la politique de sécurité entre certains segments.

```
interface BVI1
nameif inside_bvi
security-level 100
ip address 10.30.1.10 255.255.255.0
!
interface BVI2
nameif outside_bvi
security-level 0
ip address 10.40.1.10 255.255.255.0
!
interface Vlan10
bridge-group 1
nameif inside_1
security-level 100
no shutdown
!
interface Vlan20
```

```
bridge-group 2
nameif outside
security-level 0
no shutdown
!
interface Vlan30
bridge-group 1
nameif inside_2
security-level 100
no shutdown
!
interface Vlan 100
nameif dmz
security-level 0
ip address 10.1.1.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/4
switchport
switchport access vlan 20
security-level 100
no shutdown
!
interface Ethernet1/5
switchport
switchport access vlan 100
no shutdown
!
interface Ethernet1/6
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/7
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/8
switchport
switchport access vlan 100
no shutdown
```

Exemple de basculement

L'exemple suivant configure Ethernet 1/3 comme interface de basculement.

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0 standby 10.11.11.2
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0 standby 10.20.20.2
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
description LAN/STATE Failover Interface
no shutdown
!
failover
failover lan unit primary
failover lan interface folink Ethernet1/3
failover replication http
failover link folink Ethernet1/3
failover interface ip folink 10.90.90.1 255.255.255.0 standby 10.90.90.2
```

Historique des ports de commutation

Tableau 26 : Historique des ports de commutation

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge du commutateur matériel Firepower 1010	9.13(1)	L'appareil Firepower 1010 prend en charge la définition de chaque interface Ethernet comme port de commutation ou interface de pare-feu. Commandes nouvelles ou modifiées : **forward interface, interface vlan, show switch mac-address-table, show switch vlan, switchport, switchport access vlan, switchport mode, switchport trunk allowed vlan**
Prise en charge du Firepower 1010 PoE+ sur Ethernet 1/7 et Ethernet 1/8	9.13(1)	Le Firepower 1010 prend en charge Power over Ethernet+ (PoE+) sur Ethernet 1/7 et Ethernet 1/8. Commandes nouvelles ou modifiées : **power inline, show power inline**



CHAPITRE 16

Interfaces EtherChannel

Ce chapitre explique comment configurer les EtherChannels.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution système, saisissez la commande **changeto system.** .

Pour les interfaces de grappe ASA, qui ont des exigences spéciales, consultez Grappe ASA pour le Secure Firewall 3100, à la page 353.

Remarque Pour Firepower 2100 en mode plateforme et Châssis Firepower 4100/9300 , les interfaces EtherChannel sont configurées dans le système d'exploitation FXOS. Consultez le guide de configuration ou de démarrage de votre châssis pour en savoir plus.

- À propos des EtherChannels, à la page 707
- Directives pour les EtherChannels, à la page 710
- Paramètres par défaut pour les interfaces EtherChannels, à la page 712
- Configurer un EtherChannel , à la page 713
- Supervision des EtherChannels, à la page 717
- Exemples d'EtherChannels, à la page 718
- Historique des EtherChannels, à la page 718

À propos des EtherChannels

La présente section décrit les canaux EtherChannels.

About EtherChannels

Un EtherChannel 802.3ad est une interface logique (appelée interface de canal de port) composée d'un ensemble de liaisons Ethernet individuelles (un groupe de canaux), ce qui vous permet d'augmenter la bande passante pour un seul réseau. Une interface de canal de port est utilisée de la même manière qu'une interface physique lorsque vous configurez les fonctionnalités liées à l'interface.

Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces prises en charge par votre modèle.

Interfaces des groupes de canaux

Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives, sauf pour ASA, les l'ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge seulement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.

Toutes les interfaces du groupe de canaux doivent être du même type et de la même vitesse. La première interface ajoutée au groupe de canaux détermine le type et la vitesse à respecter.

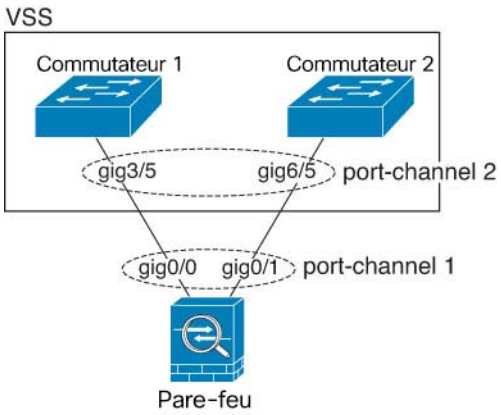
L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal. L'interface est sélectionnée à l'aide d'un algorithme de hachage exclusif, en fonction des adresses MAC source ou de destination, des adresses IP, des numéros de ports TCP et UDP et des numéros de VLAN.

Connexion à un EtherChannel sur un autre périphérique

Le périphérique auquel vous connectez l'EtherChannel ASA doit également prendre en charge l'EtherChannel 802.3ad; par exemple, vous pouvez vous connecter au commutateur Catalyst 6500 ou à Cisco Nexus 7000.

Lorsque le commutateur fait partie d'un système de commutation virtuelle (VSS) ou d'un canal de port virtuel (vPC), vous pouvez connecter des interfaces ASA dans le même EtherChannel pour séparer les commutateurs dans le VSS/vPC. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur.

Illustration 61 : Connexion à un VSS/vPC

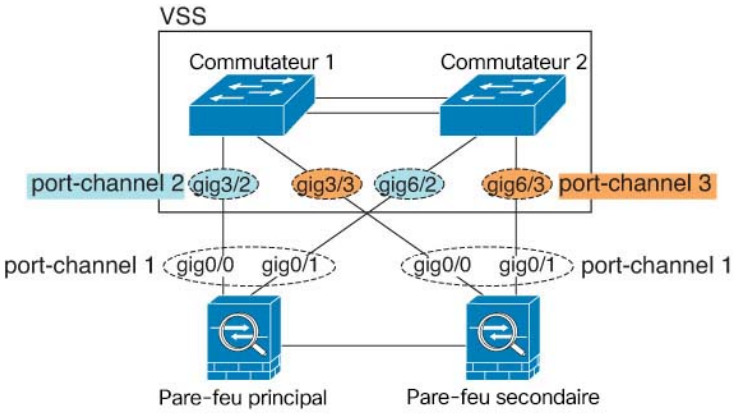


Remarque Si le périphérique ASA est en mode de pare-feu transparent et que vous placez le périphérique ASA entre deux ensembles de commutateurs VSS/vPC, veillez à désactiver la détection unidirectionnelle de liaison (UDLD) sur tous les ports de commutateur connectés au périphérique ASA avec un EtherChannel. Si vous activez UDLD, un port de commutation peut recevoir des paquets UDLD provenant des deux commutateurs de l'autre paire VSS/vPC. Le commutateur de réception place l'interface de réception à l'état inactif avec la raison « UDLD Neighbor mismatch » (Mauvaise correspondance des voisins UDLD).

Si vous utilisez le périphérique ASA dans un déploiement de basculement actif/en veille, vous devez créer des EtherChannels distincts sur les commutateurs du VSS/vPC, un pour chaque périphérique ASA. Sur chaque

périphérique ASA, un seul EtherChannel se connecte aux deux commutateurs. Même si vous pouviez regrouper toutes les interfaces de commutateur dans un seul EtherChannel qui vous connecte aux deux périphériques ASA (dans ce cas, l'EtherChannel ne sera pas établi en raison des ID de système ASA distincts), un seul EtherChannel ne serait pas souhaitable, car vous ne pouvez pas souhaitez que le trafic soit envoyé au périphérique ASA.

Illustration 62 : Basculement actif/en veille et VSS/vPC



Protocole LACP (Link Aggregation Control Protocol)

Le protocole LACP (Link Aggregation Control Protocol) agrège les interfaces en échangeant les LACPDU (Link Aggregation Control Protocol Data Unit) entre deux périphériques réseau.

Vous pouvez configurer chaque interface physique d'un EtherChannel pour qu'elle soit :

- Actif : envoie et reçoit les mises à jour du protocole LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.
- Passive : reçoit les mises à jour du protocole LACP. Un EtherChannel passif ne peut établir une connectivité qu'avec un EtherChannel actif. Non pris en charge sur les modèles matériel.
- Activé : l'EtherChannel est toujours activé et le protocole LACP n'est pas utilisé. Un EtherChannel « activé » ne peut établir une connexion qu'avec un autre EtherChannel « activé ».

Le protocole LACP coordonne l'ajout et la suppression automatiques des liens vers l'EtherChannel sans l'intervention de l'utilisateur. Il gère également les erreurs de configuration et vérifie que les deux extrémités des interfaces membres sont connectées au groupe de canaux approprié. Le mode « On » ne peut pas utiliser les interfaces en veille dans le groupe de canaux lorsqu'une interface tombe en panne et que la connectivité et les configurations ne sont pas vérifiées.

Équilibrage de la charge

Le périphérique ASA distribue les paquets aux interfaces de l'EtherChannel en hachant l'adresse IP de source et de destination du paquet (ce critère est configurable). Le hachage obtenu est divisé par le nombre de liens actifs dans une opération modulo, le reste déterminant l'interface propriétaire du flux. Tous les paquets avec un résultat *hash_value* **mod** *active_links* de 0 sont dirigés vers la première interface de l'EtherChannel, les paquets avec un résultat de 1 vont à la deuxième interface, les paquets de résultat de 2 à la troisième interface, etc. Par exemple, si vous avez 15 liens actifs, l'opération modulo fournit des valeurs de 0 à 14. Pour six liens actifs, les valeurs sont comprises entre 0 et 5, et ainsi de suite.

Pour un EtherChannel étendu en grappe, l'équilibrage de charge se produit sur une base de ASA. Par exemple, s'il y a 32 interfaces actives dans l'EtherChannel sur 8 ASA, avec 4 interfaces par ASA dans l'EtherChannel, l'équilibrage de la charge ne se produit que sur les 4 interfaces du ASA.

Si une interface active tombe en panne et n'est pas remplacée par une interface de secours, le trafic est rééquilibrage entre les liaisons restantes. La défaillance est masquée à la fois par le Spanning Tree au niveau de la couche 2 et la table de routage au niveau de la couche 3, de sorte que le basculement est transparent pour les autres périphériques du réseau.

Sujets connexes

Personnaliser l'EtherChannel (ISA 3000), à la page 715

Adresse MAC de l'EtherChannel

Toutes les interfaces qui font partie du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels.

Matériel Firepower et Cisco Secure Firewall

L'interface du canal de port utilise l'adresse MAC de l'interface interne Internal-Data 0/1. Vous pouvez également configurer manuellement une adresse MAC pour l'interface du canal de port. En mode de contexte multiple, vous pouvez affecter automatiquement des adresses MAC uniques aux interfaces *partagées*, y compris une interface de port EtherChannel. Toutes les interfaces EtherChannel d'un châssis utilisent la même adresse MAC. Sachez donc que si vous utilisez l'interrogation SNMP, par exemple, plusieurs interfaces auront la même adresse MAC.

Remarque Les interfaces membres utilisent l'adresse MAC Internal-Data 0/1 uniquement après un redémarrage. Avant de redémarrer, l'interface membre utilise sa propre adresse MAC. Si vous ajoutez une nouvelle interface membre après un redémarrage, vous devrez effectuer un autre redémarrage pour mettre à jour son adresse MAC.

Directives pour les EtherChannels

Groupe de ponts

En mode routé, les EtherChannels définis par l'ASA ne sont pas pris en charge en tant que membres du groupe de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.

Failover (basculement)

- Lorsque vous utilisez une interface EtherChannel comme lien Failover (basculement), elle doit être préconfigurée sur les deux unités de la paire Failover (basculement); vous ne pouvez pas le configurer sur l'unité principale et vous attendre à ce qu'il soit dupliquée sur l'unité secondaire, car *le lien Failover (basculement) lui-même est requis pour la duplication*.
- Si vous utilisez une interface EtherChannel , aucune configuration particulière n'est requise; la configuration peut être répliquée normalement à partir de l'unité principale. Pour le Châssis

Firepower 4100/9300 , toutes les interfaces, y compris l'EtherChannels, doivent être préconfigurées sur les deux unités.

- Vous pouvez surveiller l'EtherChannel pour Failover (basculement) à l'aide de la commande **monitor-interface**. Lorsqu'une interface membre active bascule vers une interface de secours, cette activité ne fait pas apparaître l'EtherChannel comme défaillant lors de la surveillance au niveau du périphérique Failover (basculement). Ce n'est que lorsque toutes les interfaces physiques tombent en panne que l'EtherChannel semble défaillante (pour une interface EtherChannel, le nombre d'interfaces membres autorisées à échouer peut être configuré).
- Si vous utilisez une interface EtherChannel pour un Failover (basculement) ou une liaison d'état, pour éviter les paquets dans le désordre, une seule interface de l'EtherChannel est utilisée. Si cette interface échoue, l'interface suivante de l'EtherChannel est utilisée. Vous ne pouvez pas modifier la configuration de l'EtherChannel lorsqu'elle est utilisée en tant que lien Failover (basculement). Pour modifier la configuration, vous devez désactiver temporairement Failover (basculement), ce qui empêche Failover (basculement) de se produire pendant la durée.

Prise en charge des modèles

- Vous ne pouvez pas ajouter des EtherChannels dans ASA pour le Firepower 2100 en mode plateforme, Firepower 4100/9300 ou l'ASA virtuel. Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis.
- Vous ne pouvez pas utiliser les ports de commutation ni les interfaces VLAN de Firepower 1010 dans les EtherChannels.

Mise en grappe

- Lorsque vous utilisez l'interface EtherChannel comme liaison de commande de grappe, elle doit être préconfigurée sur toutes les unités de la grappe; vous ne pouvez pas le configurer sur l'unité principale et vous attendre à ce qu'elle soit dupliquée sur les unités membres, car *la liaison de commande de grappe elle-même est requise pour la duplication*.
- Pour configurer un EtherChannel étendu ou une interface de grappe individuelle, consultez le chapitre sur la mise en grappe.

Directives générales EtherChannel

- Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces disponibles sur votre modèle.
- Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives, sauf pour ASA, les l'ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge seulement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.
- Toutes les interfaces du groupe de canaux doivent être du même type de médias et de la même capacité de vitesse, et doivent être réglées à la même vitesse et au même duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, les interfaces 1 Go et 10 Go) en réglant la vitesse pour qu'elle soit inférieure sur l'interface de plus grande capacité, sauf pour Cisco Secure Firewall

„ qui prend en charge différentes capacités d'interface à condition que la vitesse soit réglée pour détecter SFP; dans ce cas , la vitesse la plus basse est utilisée.

- Le périphérique auquel vous connectez l'EtherChannel ASA doit également prendre en charge l'EtherChannel 802.3ad.
- Le périphérique ASA ne prend pas en charge les unités LACPDU marquées VLAN. Si vous activez le balisage VLAN natif sur le commutateur voisin à l'aide de la commande Cisco IOS **vlan dot1Q tag native**, le périphérique ASA abandonnera les LACPDU balisées. Assurez-vous de désactiver le balisage VLAN natif sur le commutateur voisin. En mode de contexte multiple, ces messages ne sont pas inclus dans une capture de paquets, de sorte que vous ne pouvez pas diagnostiquer le problème facilement.
- Le débit LACP dépend du modèle. Lorsque vous définissez le débit (normal ou rapide), l'appareil demande ce débit au commutateur de connexion. En retour, l'appareil enverra au débit demandé par le commutateur de connexion. Nous vous recommandons de définir le même débit des deux côtés.
  - Firepower 4100/9300 : le débit LACPest défini sur rapide par défaut dans FXOS, mais vous pouvez le configurer comme normal (également appelé lent).
  - Cisco Secure Firewall 3100 : le débit LACP est défini sur normal (lent) par défaut, mais vous pouvez le configurer aussi rapidement sur le périphérique.
  - Tous les autres modèles : le débit LACP est défini sur normal (également appelé lent) et il n'est pas configurable, ce qui signifie que l'appareil demandera toujours un débit lent au commutateur de connexion. Nous vous recommandons de configurer le taux du commutateur sur « lent » pour que les deux côtés envoient les messages LACP au même rythme.
- Dans les versions du logiciel Cisco IOS antérieures à la 15.1(1)S2, ASA ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel ASA est connecté en pile croisée, et si le commutateur principal est mis hors tension, l'EtherChannel connecté au commutateur restant ne sera pas mis en service. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.
- Toute la configuration ASA fait référence à l'interface logique EtherChannel plutôt qu'aux interfaces physiques membres.

Paramètres par défaut pour les interfaces EtherChannels

Cette section répertorie les paramètres par défaut des interfaces si vous n'avez pas de configuration d'usine par défaut.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface et du mode de contexte.

En mode de contexte multiple, toutes les interfaces allouées sont activées par défaut, quel que soit l'état de l'interface dans l'espace d'exécution du système. Cependant, pour que le trafic passe par l'interface, celle-ci doit également être activée dans l'espace d'exécution du système. Si vous désactivez une interface dans l'espace d'exécution du système, cette interface est désactivée dans tous les contextes qui la partagent.

En mode unique ou dans l'espace d'exécution du système, les interfaces ont les états par défaut suivants :

- Interfaces physiques : désactivées.
- Interfaces de canal de port EtherChannel — Activées. Cependant, pour que le trafic passe par l'EtherChannel, les interfaces physiques des groupes de canaux doivent également être activées.

Configurer un EtherChannel

Cette section décrit comment créer une interface de canal de port EtherChannel, affecter des interfaces à l'EtherChannel et personnaliser l'EtherChannel.

Ajouter des interfaces à l'EthernetChannel

Cette section décrit comment créer une interface de canal de port EtherChannel et affecter des interfaces à l'EtherChannel. Par défaut, les interfaces de canal de port sont activées.

Avant de commencer

- Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces dont dispose votre modèle.
- Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives, sauf pour l'ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge seulement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.
- Pour configurer un EtherChannel étendu pour la mise en grappe, consultez le chapitre sur la mise en grappe au lieu de cette procédure.
- Toutes les interfaces du groupe de canaux doivent être du même type de médias et de la même capacité, et doivent être réglées sur la même vitesse et le même duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, les interfaces 1 Go et 10 Go) en réglant la vitesse pour qu'elle soit inférieure sur l'interface de plus grande capacité, sauf pour Secure Firewall 3100, qui prend en charge différentes capacités d'interface à condition que la vitesse soit réglée pour détecter SFP; dans ce cas, la vitesse la plus basse est utilisée..
- Vous ne pouvez pas ajouter d'interface physique au groupe de canaux si vous lui avez configuré un nom. Vous devez d'abord supprimer le nom à l'aide de la commande **no nameif** .
- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution système, saisissez la commande **changeto system.** .

⚠

Mise en garde Si vous utilisez une interface physique déjà présente dans votre configuration, la suppression du nom effacera toute configuration faisant référence à l'interface.

Procédure

Étape 1 Spécifiez l'interface que vous souhaitez ajouter au groupe de canaux :

interface *physical_interface*

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
```

L'ID *physical_interface* comprend le type, le logement et le numéro de port sous la forme type[slot/]port. Cette première interface du groupe de canaux détermine le type et la vitesse de toutes les autres interfaces du groupe.

En mode transparent, si vous créez un groupe de canaux avec plusieurs interfaces de gestion, vous pouvez utiliser cet EtherChannel comme interface de gestion uniquement.

Étape 2 Affectez cette interface physique à un EtherChannel :

channel-group *channel_id* **mode** {**active** | **passive** | **on**}

Exemple :

```
ciscoasa(config-if)# channel-group 1 mode active
```

Le *channel_id* est un entier compris entre 1 et 48 (1 et 8 pour les périphériques Firepower 1010). Si l'interface de canal de port pour cet ID de canal n'existe pas encore dans la configuration, elle sera ajoutée :

interface port-channel *channel_id*

Nous vous conseillons d'utiliser le mode **actif**. Le mode **passif** est uniquement disponible pour l'ISA 3000.

Étape 3 (Facultatif) (Secure Firewall 3100 uniquement) Définit le débit de réception de l'unité de données LACP pour une interface physique dans le groupe de canaux.

lacp rate {**normal** | **fast**}

La valeur par défaut est de **normal** (lent, toutes les 30 secondes). L'option **fast** reçoit des unités de données LACP chaque seconde. Vous devez faire correspondre le paramètre sur le commutateur connecté.

Étape 4 (Facultatif) (ModèlesISA 3000 uniquement) Définissez la priorité d'une interface physique dans le groupe de canaux.

lacp port-priority *number*

Exemple :

```
ciscoasa(config-if)# lacp port-priority 12345
```

Le *numéro* de priorité est un entier compris entre 1 et 65535. La valeur par défaut est 32768. Plus le numéro de priorité est élevé, plus la priorité est faible. L'ASA utilise ce paramètre pour décider quelles interfaces sont actives et lesquelles sont en veille si vous attribuez plus d'interfaces que ce qui peut être utilisé. Si le paramètre de priorité de port est le même pour toutes les interfaces, la priorité est déterminée par l'ID d'interface

(logement/port). L'ID d'interface le plus faible correspond à la priorité la plus élevée. Par exemple, GigabitEthernet 0/0 est une priorité plus élevée que GigabitEthernet 0/1.

Si vous souhaitez donner la priorité à une interface pour qu'elle soit active même si elle a un ID d'interface plus élevé, définissez cette commande pour avoir une valeur inférieure. Par exemple, pour rendre actif GigabitEthernet 1/3 avant GigabitEthernet 0/7, faites que la valeur **lacp port-priority** soit de 12345 sur l'interface 1/3 contre la valeur par défaut de 32768 sur l'interface 0/7.

Si le périphérique à l'autre extrémité de l'EtherChannel a des priorités de port conflictuelles, la priorité du système est utilisée pour déterminer les priorités de port à utiliser. Reportez-vous à la commande **lacp system-priority**.

Étape 5 (Facultatif) Définissez les propriétés Ethernet de l'interface de canal de port pour remplacer les propriétés définies sur les interfaces individuelles.

interface port-channel *channel_id*

Consultez Activer l'interface physique et configurer les paramètres Ethernet, à la page 675 pour les commandes Ethernet. Cette méthode offre un raccourci pour définir ces paramètres, car ceux-ci doivent correspondre pour toutes les interfaces du groupe de canaux.

Étape 6 Répétez les étapes 1 à 3 pour chaque interface que vous souhaitez ajouter au groupe de canaux.

Chaque interface du groupe de canaux doit être du même type et avoir la même vitesse. Le mode semi-duplex n'est pas pris en charge. Si vous ajoutez une interface qui ne correspond pas, elle sera mise à l'état suspendu.

Étape 7 (Facultatif) (Secure Firewall 3100 uniquement) Définit le débit de réception de l'unité de données LACP pour une interface physique dans le groupe de canaux.

a) Cliquez sur l'interface physique dans le tableau **Interfaces**, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche.

b) Cliquez sur l'onglet **Advanced (Avancé)**.

c) Dans la zone **EtherChannel**, dans la liste déroulante **Rate** (Débit), choisissez **Normal** ou **Fast** (Rapide).

La valeur par défaut est **Normal** (lent, toutes les 30 secondes). L'option **Fast** (Rapide) reçoit des mises à jour LACP chaque seconde. Vous devez faire correspondre le paramètre sur le commutateur connecté.

Sujets connexes

Protocole LACP (Link Aggregation Control Protocol), à la page 709
Personnaliser l'EtherChannel (ISA 3000), à la page 715

Personnaliser l'EtherChannel (ISA 3000)

Cette section décrit comment définir le nombre maximal d'interfaces dans l'EtherChannel, le nombre minimal d'interfaces opérationnelles pour que l'EtherChannel soit actif, l'algorithme d'équilibrage de charges et d'autres paramètres facultatifs. Ces paramètres ne s'appliquent qu'aux ISA 3000.

Procédure

Étape 1 Spécifiez l'interface de canal de port :

interface port-channel *channel_id*

Exemple :

```
ciscoasa(config)# interface port-channel 1
```

Cette interface a été créée automatiquement lorsque vous avez ajouté une interface au groupe de canaux. Si vous n'avez pas encore ajouté d'interface, cette commande crée l'interface de canal de port.

Vous devez ajouter au moins une interface membre à l'interface de canal de port avant de pouvoir configurer ses paramètres logiques, comme un nom.

Étape 2 Spécifiez le nombre maximal d'interfaces actives autorisées dans le groupe de canaux :

lacp max-bundle *number*

Exemple :

```
ciscoasa(config-if)# lacp max-bundle 6
```

Le *nombre* est compris entre 1 et 16. Par défaut, c'est 16. Si votre commutateur ne prend pas en charge 16 interfaces actives, veillez à régler cette commande à 8 ou moins.

Étape 3 Spécifiez le nombre minimal d'interfaces actives requises pour que l'interface de canal de port devienne active :

port-channel min-bundle *number*

Exemple :

```
ciscoasa(config-if)# port-channel min-bundle 2
```

Le *nombre* est compris entre 1 et 16. La valeur par défaut est 1. Si le nombre d'interfaces actives dans le groupe de canaux tombe en dessous de cette valeur, l'interface de canal de port est désactivée, ce qui peut déclencher un basculement au niveau du périphérique.

Étape 4 Configurez l'algorithme d'équilibrage de charges :

port-channel load-balance {**dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port**}

Exemple :

```
ciscoasa(config-if)# port-channel load-balance src-dst-mac
```

Par défaut, l'ASA équilibre la charge de paquets sur les interfaces en fonction de l'adresse IP source et de destination (**src-dst-ip**) du paquet. Si vous souhaitez modifier les propriétés selon lesquelles le paquet est classé, utilisez cette commande. Par exemple, si votre trafic est fortement orienté vers les mêmes adresses IP de source et de destination, l'affectation du trafic aux interfaces de l'EtherChannel ne sera pas équilibrée. Le passage à un algorithme différent peut entraîner une répartition plus uniforme du trafic.

Étape 5 Définissez la priorité du système LACP :

lacp system-priority *number*

Exemple :

```
ciscoasa(config)# lacp system-priority 12345
```

Le *nombre* est compris entre 1 et 65535. La valeur par défaut est 32768. Plus le numéro de priorité est élevé, plus la priorité est faible. Cette commande est globale pour l'ASA.

Si le périphérique à l'autre extrémité de l'EtherChannel a des priorités de port conflictuelles, la priorité du système est utilisée pour déterminer les priorités de port à utiliser. Pour les priorités d'interface dans un EtherChannel, consultez la commande **lacp port-priority**.

Sujets connexes

Équilibrage de la charge, à la page 709
Ajouter des interfaces à l'EthernetChannel, à la page 713

Supervision des EtherChannels

Consultez les commandes suivantes :

Remarque Pour les modèles Firepower et Secure Firewall, certaines statistiques ne sont pas affichées à l'aide des commandes ASA. Vous devez consulter des statistiques d'interface plus détaillées à l'aide des commandes FXOS.

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

Pour Firepower 2100 en mode plateforme, consultez aussi les commandes FXOS connect local-mgmt suivantes :

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

Consultez le guide de dépannage FXOS pour plus d'informations.

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

- (ISA 3000 uniquement) **show lacp** {[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}

  Pour EtherChannel, affiche les renseignements LACP tels que les statistiques de trafic, l'identifiant du système et les détails du voisin.

- (ISA 3000 uniquement) **show port-channel** [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

  Pour EtherChannel, affiche les renseignements sur EtherChannel dans un récapitulatif détaillé et sur une ligne. Cette commande affiche également les renseignements sur le port et le canal de port.

- (ISA 3000 uniquement) **show port-channel** *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **l4port** | **mac** | **mixed** | **vlan-only**} *parameters*]

  Pour EtherChannel, affiche les renseignements sur l'équilibrage de charges du canal de port, ainsi que le résultat du hachage et l'interface membre sélectionnée pour un ensemble de paramètres donné.

Exemples d'EtherChannels

L'exemple suivant configure trois interfaces dans le cadre d'un EtherChannel. Il définit également la priorité système pour une priorité plus élevée et GigabitEthernet 0/2 pour une priorité plus élevée que les autres interfaces dans le cas où plus de huit interfaces sont affectées à l'EtherChannel.

```
lacp system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
  lacp port-priority 1234
  channel-group 1 mode passive
interface Port-channel1
  lacp max-bundle 4
  port-channel min-bundle 2
  port-channel load-balance dst-ip
```

Historique des EtherChannels

Tableau 27 : Historique des EtherChannels

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge EtherChannel	v 8.4(1)	Vous pouvez configurer jusqu'à 48 EtherChannels 802.3ad de huit interfaces actives chacun. Nous avons introduit les commandes suivantes : **channel-group**, **lacp port-priority**, **interface port-channel**, **lacp max-bundle**, **port-channel min-bundle**, **port-channel load-balance**, **lacp system-priority**, **clear lacp counters**, **show lacp**, **show port-channel**. **Remarque** EtherChannel n'est pas pris en charge sur l'ASA 5505.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de 16 liens actifs dans un EtherChannel	9.2(1)	Vous pouvez maintenant configurer jusqu'à 16 liens actifs dans un EtherChannel. Auparavant, vous pouviez avoir 8 liens actifs et 8 liens de secours. Assurez-vous que votre commutateur peut prendre en charge 16 liens actifs (par exemple, Cisco Nexus 7000 avec module F2-Series 10 Gigabit Ethernet). **Remarque** Si vous effectuez une mise à niveau à partir d'une version antérieure d'ASA, le nombre maximum d'interfaces actives est défini sur 8 à des fins de compatibilité (commande **lacp max-bundle**). Nous avons modifié les commandes suivantes : **lacp max-bundle** and **port-channel min-bundle**.



CHAPITRE 17

Interfaces de boucle avec retour

Ce chapitre explique comment configurer les interfaces de boucle avec retour.

- À propos des interfaces de boucle avec retour, à la page 721
- Directives pour les interfaces de boucle avec retour, à la page 722
- Configurer une interface de boucle avec retour, à la page 722
- Limite de débit du trafic vers l'interface de boucle avec retour, à la page 722
- Supervision des interfaces de boucle avec retour, à la page 724
- Historique des interfaces de boucle avec retour, à la page 724

À propos des interfaces de boucle avec retour

Une interface de boucle avec retour est une interface logicielle uniquement qui émule une interface physique. Cette interface est accessible sur IPv4 et IPv6 par l'intermédiaire de plusieurs interfaces physiques. L'interface de boucle avec retour permet de résoudre les échecs de chemin. elle est accessible à partir de n'importe quelle interface physique. Par conséquent, si l'une d'elles tombe en panne, vous pouvez accéder à l'interface de boucle avec retour à partir d'une autre.

Les interfaces de boucle avec retour peuvent être utilisées pour :

- AAA
- BGP
- SNMP
- SSH
- Tunnels VTI statiques et dynamiques
- Syslog
- Telnet

Le ASA peut distribuer l'adresse de boucle avec retour à l'aide de protocoles de routage dynamique, ou vous pouvez configurer une voie de routage statique sur le périphérique homologue pour atteindre l'adresse IP de boucle avec retour par l'une des interfaces physiques de ASA. Vous ne pouvez pas configurer une voie de routage statique sur ASA qui spécifie l'interface de boucle avec retour.

Directives pour les interfaces de boucle avec retour

Failover (basculement) et mise en grappe

- Aucune prise en charge de mise en grappe.

Mode contextuel

- Le VTI est pris en charge en mode de contexte unique uniquement. Les autres utilisations de la boucle avec retour sont prises en charge en mode contexte multiple.

Directives et limites additionnelles

- La répartition aléatoire des séquences TCP est toujours désactivée pour le trafic de l'interface physique à l'interface de boucle avec retour.

Configurer une interface de boucle avec retour

Ajoutez une interface de boucle avec retour.

Procédure

Étape 1 Créez une interface de boucle avec retour :

interface loopback *number*

Le nombre peut être compris entre 0 et 10413.

Exemple :

```
ciscoasa(config)# interface loopback 10
```

Étape 2 Configurez le nom et l'adresse IP. Consultez Interfaces en mode routage et en mode transparent, à la page 763

Étape 3 Configurez la limitation de débit pour le trafic de boucle avec retour. Consultez Limite de débit du trafic vers l'interface de boucle avec retour, à la page 722.

Limite de débit du trafic vers l'interface de boucle avec retour

Vous devez limiter le trafic vers l'adresse IP de l'interface de boucle avec retour pour éviter une charge excessive sur le système. Vous pouvez ajouter une règle de limite de connexion à la politique de service globale. Cette procédure montre l'ajout à la politique globale par défaut (global_policy).

Procédure

Étape 1 Créez une liste d'accès identifiant le trafic vers l'adresse IP de l'interface de boucle avec retour.

access-list *name* **extended permit ip any host** *loopback_ip*

Créez un ACE pour chaque adresse IP d'interface de boucle avec retour. Vous pouvez également restreindre cette liste d'accès en spécifiant les adresses IP source plutôt que **any** (toute).

Exemple :

```
ciscoasa(config)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
```

Étape 2 Créez une carte de trafic qui identifie la liste d'accès.

class-map *name*

match access-list *acl_name*

Exemple :

```
ciscoasa(config)# class-map rate-limit-loopback
ciscoasa(config-cmap)# match access-list loop
```

Étape 3 Appliquez le nombre maximum de connexions et de connexions amorces à la carte de trafic dans le cadre de la liste des politiques globales.

policy-map global_policy

class *class_map_name*

set connection conn-max *conns* **embryonic-conn-max** *conns*

Définissez le nombre maximum de connexions sur le nombre attendu de connexions pour l'interface de boucle avec retour et le nombre de connexions amorces à un nombre inférieur. Par exemple, vous pouvez lui régler la valeur 5/2, 10/5 ou 1024/512, selon le nombre de sessions d'interface de boucle avec retour attendues dont vous avez besoin.

La définition de la limite de connexions amorces active l'interception de TCP, qui protège le système contre une attaque DoS perpétrée en inondant une interface de paquets SYN de TCP.

Exemple :

```
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class rate-limit-loopback
ciscoasa(config-pmap-c)# set connection conn-max 5 embryonic-conn-max 2
```

Exemple

L'exemple suivant définit le nombre maximum de connexions et de connexions amorces à 10 et 5 pour la politique globale par défaut pour tout le trafic allant à deux interfaces de boucle avec retour à l'adresse 10.1.1.1 et 10.2.1.1.

```
ciscoasa(config)# interface loopback 1
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop1
ciscoasa(config-if)# interface loopback 2
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop2
ciscoasa(config-if)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match access-list loop
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection conn-max 10 embryonic-conn-max 5
```

Supervision des interfaces de boucle avec retour

Consultez les commandes suivantes :

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

Historique des interfaces de boucle avec retour

Tableau 28 : Historique des interfaces de boucle avec retour

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge de l'interface de boucle avec retour pour VTI	9.19(1)	Une interface de boucle avec retour fournit la redondance des tunnels VPN VTI statiques et dynamiques. Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. L'interface VTI peut également hériter de l'adresse IP d'une interface de boucle avec retour au lieu d'une adresse IP configurée de manière statique. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP de l'interface de boucle avec retour. Commandes nouvelles/modifiées : **tunnel source interface**, **ip unnumbered**, **ipv6 unnumbered**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge de l'interface de boucle avec retour	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour : • BGP • AAA • SNMP • Journal système • SSH • Telnet Commandes nouvelles ou modifiées : **interface loopback**, **logging host**, **neighbor update-source**, **snmp-server host**, **ssh**, **telnet**



CHAPITRE 18

Sous-interfaces VLAN

Ce chapitre explique comment configurer les sous-interfaces VLAN.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

- À propos des sous-interfaces VLAN, à la page 727
- Licences pour les sous-interfaces VLAN, à la page 727
- Lignes directrices et limites pour les sous-interfaces VLAN, à la page 728
- Paramètres par défaut pour les sous-interfaces VLAN, à la page 729
- Configurer les sous-interfaces VLAN et la jonction 802.1Q, à la page 729
- Supervision des sous-interfaces VLAN, à la page 731
- Exemples de sous-interfaces VLAN, à la page 731
- Historique des sous-interfaces VLAN, à la page 732

À propos des sous-interfaces VLAN

Les sous-interfaces VLAN vous permettent de diviser une interface physiqueou EtherChannel en plusieurs interfaces logiques qui sont étiquetées avec différents ID de VLAN. Une interface avec une ou plusieurs sous-interfaces VLAN est automatiquement configurée comme une ligne principale 802.1Q. Comme les réseaux VLAN vous permettent de garder le trafic séparé sur une interface physique donnée, vous pouvez augmenter le nombre d'interfaces disponibles pour votre réseau sans ajouter d'interfaces physiques ou d'ASA supplémentaires. Cette fonctionnalité est particulièrement utile en mode de contexte multiple, car vous pouvez affecter des interfaces uniques à chaque contexte.

Vous pouvez configurer un VLAN principal ainsi qu'un ou plusieurs VLAN secondaires. Lorsque l'ASA reçoit le trafic sur les VLAN secondaires, il le mappe au VLAN principal.

Licences pour les sous-interfaces VLAN

Modèle	Exigence de licence
Firepower 1010	Licence Essentials : 60

Modèle	Exigence de licence
Firepower 1120	Licence Essentials : 512
Firepower 1140, 1150	Licence Essentials : 1 024
Firepower de la série 2100	Licence Essentials : 1 024
Secure Firewall 3100	Licence Essentials : 1 024
Firepower 4100	Licence Essentials : 1 024
Firepower 9300	Licence Essentials : 1 024
ASA virtuel	Capacité de débit : 100 Mbit/s : 25 1 Gbit/s : 50 2 Gbit/s : 200 10 Gbit/s : 1 024
ISA 3000	LicenceEssentials : 5 Licence Security Plus : 100

Remarque Pour qu'une interface soit prise en compte dans la limite de VLAN, vous devez lui attribuer un VLAN.Par exemple :

```
interface gigabitethernet 0/0.100
  vlan 100
```

Lignes directrices et limites pour les sous-interfaces VLAN

Prise en charge des modèles

- Firepower 1010 : les sous-interfaces VLAN ne sont pas prises en charge sur les ports de commutation ou les interfaces VLAN.
- Pour la des modèles ASA, vous ne pouvez pas configurer de sous-interface sur l'interface de gestion. Consultez L'interface de logement/port de gestion, à la page 672 pour la prise en charge des sous-interfaces.

Directives supplémentaires

- Prévention des paquets non balisés sur l'interface physique : Si vous utilisez des sous-interfaces, vous ne souhaitez généralement pas que l'interface physique achemine le trafic, car l'interface physique peut transmettre des paquets non balisés. Cette propriété est également vraie pour l'interface physique active

pour les liaisons EtherChannel. Étant donné que l'interface physique ou EtherChannel doit être activée pour que la sous-interface achemine le trafic, assurez-vous que l'interface physique ou EtherChannel ne transmet pas le trafic en omettant la commande **nameif**. Si vous voulez laisser l'interface physique ou EtherChannel passer des paquets non balisés, vous pouvez configurer la commande **nameif** comme d'habitude.

- Toutes les sous-interfaces de la même interface parente doivent soit être des membres de groupes de ponts, soit des interfaces routées; vous ne pouvez pas combiner les deux types.
- L'ASA ne prend pas en charge le protocole DTP (Dynamic Trunking Protocol), vous devez donc configurer le port de commutation connectée pour qu'il assure la liaison sans condition.
- Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur l'ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur ASA. Vous pouvez générer automatiquement des adresses MAC uniques; voir Attribuer automatiquement des adresses MAC, à la page 808.



Remarque Si vous attribuez manuellement une adresse MAC, veillez à attribuer des adresses MAC à toutes les sous-interfaces sur la même interface physique pour éviter les comportements imprévus et les pannes.

Paramètres par défaut pour les sous-interfaces VLAN

Cette section répertorie les paramètres par défaut des interfaces si vous n'avez pas de configuration d'usine par défaut.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface et du mode de contexte.

En mode de contexte multiple, toutes les interfaces allouées sont activées par défaut, quel que soit l'état de l'interface dans l'espace d'exécution du système. Cependant, pour que le trafic passe par l'interface, celle-ci doit également être activée dans l'espace d'exécution du système. Si vous désactivez une interface dans l'espace d'exécution du système, cette interface est désactivée dans tous les contextes qui la partagent.

En mode unique ou dans l'espace d'exécution du système, les interfaces ont les états par défaut suivants :

- Interfaces physiques : désactivées.
- Sous-interfaces VLAN : activées. Cependant, pour que le trafic passe par la sous-interface, l'interface physique doit également être activée.

Configurer les sous-interfaces VLAN et la jonction 802.1Q

Ajoutez une sous-interface VLAN à une interface physique ou EtherChannel.

Avant de commencer

Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Spécifiez la nouvelle sous-interface :

interface {*physical_interface* | **port-channel** *number*}.*subinterface*

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

L'argument **port-channel** *number* est l'ID de l'interface EtherChannel, tel que **port-channel 1**.

L'ID de la *sous-interface* est un nombre entier compris entre 1 et 4294967293.

Étape 2 Spécifiez le VLAN de la sous-interface :

vlan *vlan_id* [**secondary** *vlan_range*]

Exemple :

```
ciscoasa(config-subif)# vlan 101 secondary 52 64,66-74
```

Le *vlan_id* est un entier compris entre 1 et 4094. Certains numéros de VLAN peuvent être réservés sur les commutateurs connectés. Consultez la documentation du commutateur pour en savoir plus.

Les réseaux VLAN secondaires peuvent être séparés par des espaces, des virgules et des tirets (pour une plage contiguë). Lorsque l'ASA reçoit le trafic sur les VLAN secondaires, il mappe le trafic au VLAN principal.

Vous ne pouvez pas attribuer le même réseau VLAN à plusieurs sous-interfaces. Vous ne pouvez pas attribuer de réseau VLAN à l'interface physique. Chaque sous-interface doit avoir un ID VLAN avant de pouvoir transmettre du trafic. Pour modifier un ID VLAN, vous n'avez pas besoin de supprimer l'ancien ID VLAN avec l'option **no** (non); vous pouvez saisir la commande **vlan** avec un autre ID VLAN et l'ASA modifie l'ancien ID. Pour supprimer certains VLAN secondaires de la liste, vous pouvez utiliser la commande **no** (non) et répertorier uniquement les VLAN à supprimer. Vous pouvez uniquement supprimer de manière sélective les VLAN répertoriés; vous ne pouvez pas supprimer un seul VLAN dans une plage, par exemple.

Exemples

L'exemple suivant mappe un ensemble de VLAN secondaires au VLAN 200 :

```
interface gigabitethernet 0/6.200
   vlan 200 secondary 500 503 600-700
```

Dans l'exemple suivant, le VLAN 503 secondaire est supprimé de la liste :

```
no vlan 200 secondary 503
```

```
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
 vlan 200 secondary 500 600-700
 no nameif
 no security-level
 no ip address
```

Sujets connexes

Licences pour les sous-interfaces VLAN, à la page 727

Supervision des sous-interfaces VLAN

Consultez les commandes suivantes :

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

- **show vlan mapping**

  Affiche l'interface, les VLAN secondaires et les VLAN principaux auxquels ils sont mappés.

Exemples de sous-interfaces VLAN

L'exemple suivant configure les paramètres d'une sous-interface en mode unique :

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

L'exemple suivant montre comment le mappage de VLAN fonctionne avec le commutateur Catalyst 6500. Consultez le guide de configuration du commutateur Catalyst 6500 pour savoir comment connecter des nœuds à des PVLAN.

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
```

```
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 Configuration

```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

Historique des sous-interfaces VLAN

Tableau 29 : Historique des sous-interfaces VLAN

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Augmentation du nombre de VLAN	7.0(5)	Augmentation des limites suivantes : • VLAN de licences de base ASA 5510 de 0 à 10. • VLAN de licences Security Plus ASA 5510, 10 à 25. • VLAN ASA 5520 de 25 à 100. • VLAN ASA 5540 de 100 à 200.
Augmentation du nombre de VLAN	7.2(2)	Les limites de VLAN ont été augmentées pour l'ASA 5510 (de 10 à 50 pour la licence de base et de 25 à 100 pour la licence Security Plus), l'ASA 5520 (de 100 à 150), l'ASA 5550 (de 200 à 250).
Augmentation du nombre de VLAN pour l'ASA 5580	8.1(2)	Le nombre de VLAN pris en charge sur l'ASA 5580 est passé de 100 à 250.

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge du mappage d'un VLAN secondaire à un VLAN principal	9.5(2)	Vous pouvez maintenant configurer un ou plusieurs VLAN secondaires pour une sous-interface. Lorsque l'ASA reçoit le trafic sur les VLAN secondaires, il le mappe au VLAN principal. Nous avons introduit ou modifié les commandes suivantes : **vlan secondary, show vlan mapping**
Augmentation du nombre de VLAN pour l'ISA 3000	9.13(1)	Le nombre maximum de VLAN pour l'ISA 3000 avec la licence Security Plus est passé de 25 à 100.



CHAPITRE 19

Interfaces VXLAN

Ce chapitre explique comment configurer des interfaces Virtual eXtensible LAN (VXLAN). Les VXLAN agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3 pour étendre les réseaux de couche 2.

- À propos des interfaces VXLAN, à la page 735
- Exigences et conditions préalables pour les interfaces VXLAN, à la page 743
- Lignes directrices pour les interfaces VXLAN, à la page 743
- Paramètres par défaut des interfaces VXLAN, à la page 744
- Configurer les interfaces VXLAN, à la page 745
- Configurer les interfaces Geneve, à la page 750
- Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle, à la page 753
- Supervision des interfaces VXLAN, à la page 755
- Exemples d'interfaces VXLAN, à la page 757
- Historique des interfaces VXLAN, à la page 761

À propos des interfaces VXLAN

Le réseau VXLAN fournit les mêmes services de réseau Ethernet de couche 2 que le réseau VLAN, mais avec une extensibilité et une flexibilité accrues. Par rapport au VLAN, le VXLAN offre les avantages suivants :

- Emplacement flexible des segments multidétenteurs dans le centre de données.
- Évolutivité accrue pour traiter un plus grand nombre de segments de couche 2 : jusqu'à 16 millions de segments VXLAN.

Cette section décrit le fonctionnement de VXLAN. Pour en savoir plus sur VXLAN, consultez RFC 7348. Pour des informations détaillées sur Geneve, consultez RFC 8926.

Encapsulation

L'ASA prend en charge deux types d'encapsulation VXLAN :

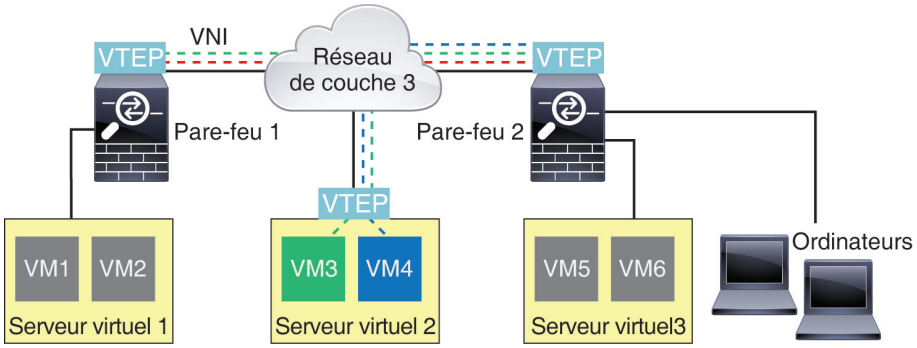
- VXLAN (tous les modèles) : VXLAN utilise l'encapsulation MAC Address-in-User Datagram Protocol (MAC-in-UDP). Un en-tête VXLAN est ajouté à la trame de couche 2 d'origine, qui est ensuite placée dans un paquet UDP-IP.

- Geneve (ASA virtuel uniquement) : Geneve a un en-tête interne flexible qui ne se limite pas à l'adresse MAC. L'encapsulation Geneve est requise pour un routage transparent des paquets entre un équilibreur de charge de passerelle Amazon Web Services (AWS) et les périphériques, et pour l'envoi d'informations supplémentaires.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP a deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier) auxquelles vous appliquez votre politique de sécurité, et une interface normale appelée l'interface source VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

La figure suivante montre deux ASA et le serveur virtuel 2 agissant comme des VTEP dans un réseau de couche 3 et étendant les réseaux VNI 1, 2 et 3 entre les sites. Les ASA agissent comme des ponts ou des passerelles entre les réseaux VXLAN et les non-VXLAN.



Le réseau IP sous-jacent entre les VTEP est indépendant de la superposition VXLAN. Les paquets encapsulés sont acheminés en fonction de l'en-tête d'adresse IP externe, qui a le VTEP de départ comme adresse IP source et le VTEP de fin comme adresse IP de destination. Pour l'encapsulation VXLAN : l'adresse IP de destination peut être un groupe de multidiffusion lorsque le VTEP distant est inconnu. Avec Geneve, l'ASA ne prend en charge que les homologues statiques. Le port de destination de VXLAN est le port UDP 4789 par défaut (configurable par l'utilisateur). Le port de destination pour Geneve est le 6081.

Interface de la source VTEP

L'interface source de VTEP est une interface ASA normale (physique, EtherChannel ou même VLAN) à laquelle vous prévoyez d'associer toutes les interfaces VNI. Vous pouvez configurer une interface source de VTEP par ASA ou contexte de sécurité. Comme vous ne pouvez configurer qu'une seule interface source de VTEP, vous ne pouvez pas configurer les deux interfaces VXLAN et Geneve sur le même périphérique.Il y a une exception pour la mise en grappe d'ASA virtuel sur AWS, où vous pouvez avoir deux interfaces sources VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe, et une interface Geneve peut être utilisée pour l'équilibreur de charges de la passerelle.

L'interface source de VTEP peut être entièrement dédiée au trafic VXLAN, bien qu'elle ne se limite pas à cet usage. Si vous le souhaitez, vous pouvez utiliser l'interface pour le trafic normal et appliquer une politique de sécurité à l'interface pour ce trafic. Pour le trafic VXLAN, cependant, toute la politique de sécurité doit être appliquée aux interfaces VNI. L'interface VTEP sert uniquement de port physique.

En mode de pare-feu transparent, l'interface source de VTEP ne fait pas partie d'un BVI, et vous configurez une adresse IP pour elle, similaire à la façon dont l'interface de gestion est traitée.

Interface VNIs

Les interfaces VNI sont similaires aux interfaces VLAN : ce sont des interfaces virtuelles qui séparent le trafic réseau sur une interface physique donnée en utilisant le balisage. Vous appliquez votre politique de sécurité directement à chaque interface VNI.

Vous ne pouvez ajouter qu'une seule interface VTEP et toutes les interfaces VNI sont associées à la même interface VTEP.Il existe une exception pour la mise en grappe d'ASA virtuel sur AWS. Pour la mise en grappe d'AWS, vous pouvez avoir deux interfaces source VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe et une interface Geneve peut être utilisée pour AWS Gateway Load Balancer.

Traitement de paquet VXLAN

VXLAN

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement VXLAN, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête VXLAN.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.
- L'adresse IP de destination de la trame externe est déterminée par une recherche IP distante du VTEP.

Désencapsulation : l'ASA désencapsule un paquet VXLAN uniquement dans les cas suivants :

- Il s'agit d'un paquet UDP dont le port de destination est 4789 (cette valeur peut être configurée par l'utilisateur).
- L'interface d'entrée est l'interface source du VTEP.
- L'adresse IP de l'interface d'entrée est la même que l'adresse IP de destination.
- Le format des paquets VXLAN est conforme à la norme.

Geneve

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement de Geneve, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête Geneve.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.

- L’adresse IP de destination de la trame externe est définie sur l’adresse IP homologue que vous avez configurée.

Désencapsulation : l’ASA désencapsule un paquet Geneve uniquement dans les cas suivants :

- Il s’agit d’un paquet UDP dont le port de destination est 6081 (cette valeur peut être configurée par l’utilisateur).
- L’interface d’entrée est l’interface source du VTEP.
- L’adresse IP de l’interface d’entrée est la même que l’adresse IP de destination.
- Le format des paquets Geneve est conforme à la norme.

Pair VTEP

Lorsque l’ASA envoie un paquet à un périphérique derrière un VTEP homologue, l’ASA a besoin de deux renseignements importants :

- L’adresse MAC de destination du périphérique distant
- L’adresse IP de destination du VTEP homologue

L’ASA gère un mappage des adresses MAC de destination sur les adresses IP du VTEP distant pour les interfaces VNI.

Homologue VXLAN

L’ASA peut trouver ces renseignements de deux manières :

- Une adresse IP VTEP homologue unique peut être configurée de manière statique sur l’ASA.

  Vous ne pouvez pas définir manuellement plusieurs homologues.

  L’ASA envoie ensuite une diffusion ARP encapsulée dans VXLAN au VTEP pour connaître l’adresse MAC du nœud d’extrémité.

- Un groupe de multidiffusion peut être configuré sur chaque interface VNI (ou sur le VTEP dans son ensemble).

Remarque Cette option n’est pas prise en charge par Geneve.

: l’ASA envoie un paquet de diffusion ARP encapsulé dans VXLAN dans un paquet IP de multidiffusion par l’intermédiaire de l’interface source de VTEP. La réponse à cette requête ARP permet à l’ASA d’apprendre à la fois l’adresse IP du VTEP distant ainsi que l’adresse MAC de destination du nœud d’extrémité distant.

Homologue Geneve

L’ASA virtuel ne prend en charge que les homologues définis de manière statique. Vous pouvez définir l’adresse IP homologue ASA virtuel sur l'équilibreur de charge de passerelle AWS. Comme l’ASA virtuel n’initie jamais le trafic vers l’équilibreur de charges de passerelle, vous n’avez pas besoin de préciser l’adresse

IP de l'équilibreur de charges de passerelle sur l'ASA virtuel; il connaît l'adresse IP homologue lorsqu'il reçoit le trafic de Geneve. Les groupes de multidiffusion ne sont pas pris en charge avec Geneve.

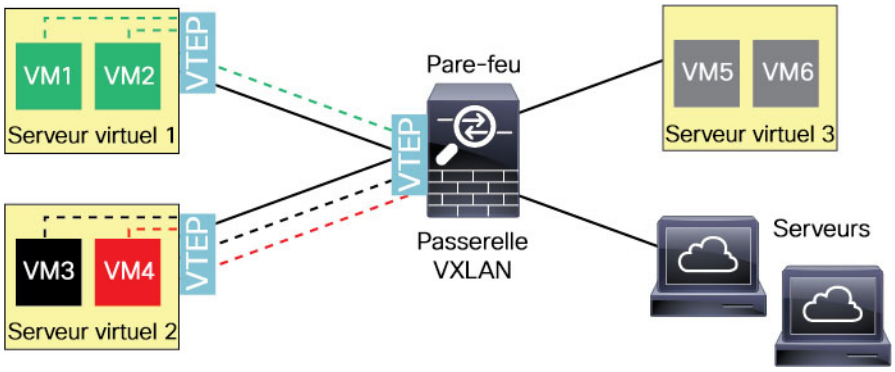
Scénarios VXLAN

Cette section décrit les scénarios d'utilisation de la mise en œuvre de VXLAN sur l'ASA.

Présentation du pont ou de la passerelle VXLAN

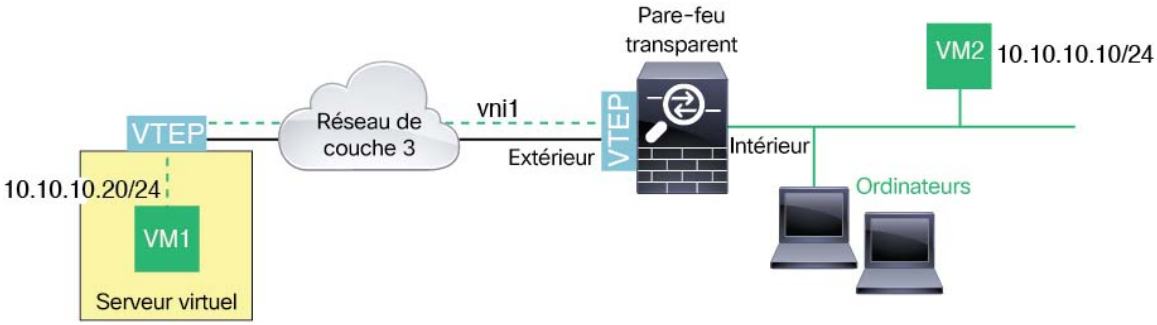
Chaque VTEP ASA agit comme un pont ou une passerelle entre les nœuds terminaux comme les machines virtuelles, les serveurs et les PC et le réseau de superposition VXLAN. Pour les trames entrantes reçues avec encapsulation VXLAN sur l'interface source de VTEP, ASA supprime l'en-tête VXLAN et le transfère vers une interface physique connectée à un réseau non VXLAN en fonction de l'adresse MAC de destination de la trame Ethernet interne.

L'ASA traite toujours les paquets VXLAN; il ne se contente pas de transférer des paquets VXLAN inchangés entre deux autres VTEP.



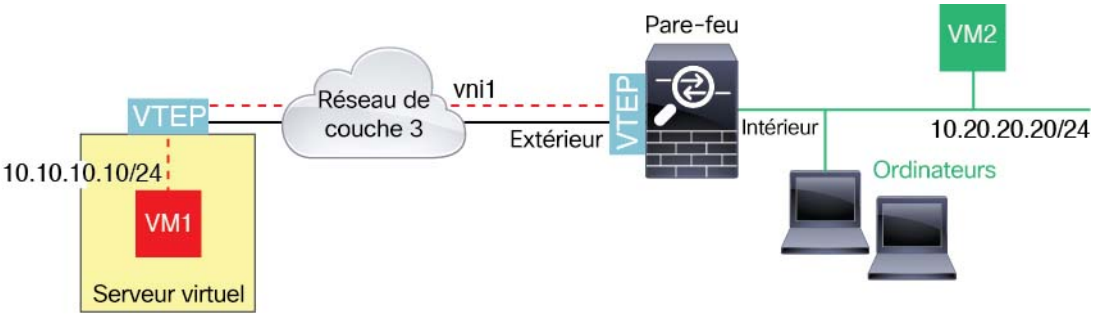
Pont VXLAN

Lorsque vous utilisez un groupe de ponts (mode de pare-feu transparent ou mode de routage facultatif), ASA peut servir de pont VXLAN entre un segment VXLAN (distant) et un segment local, où les deux se trouvent dans le même réseau. Dans ce cas, un membre du groupe de ponts est une interface standard tandis que l'autre membre est une interface VNI.



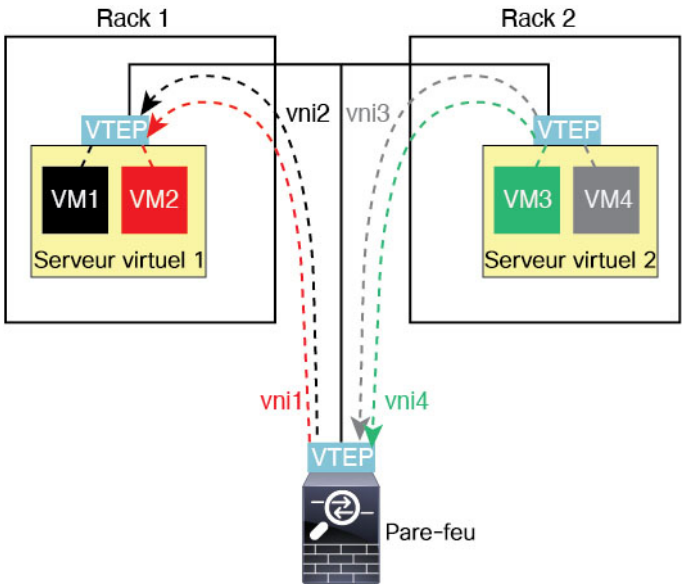
Passerelle VXLAN (mode routé)

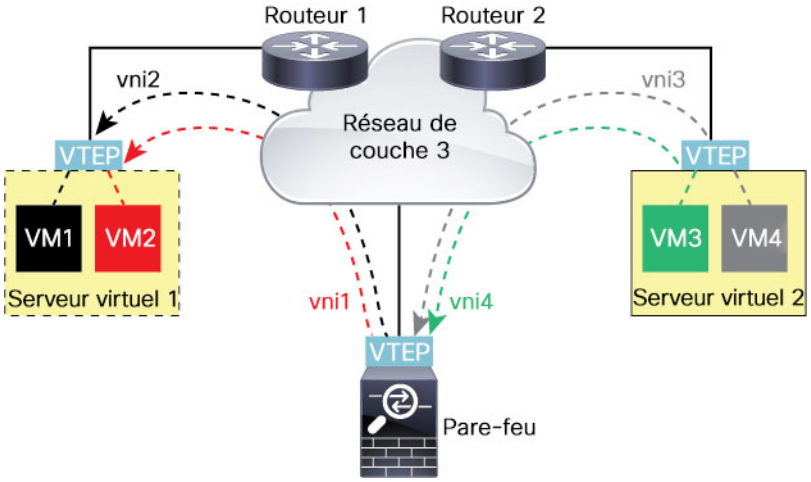
L'ASA peut servir de routeur entre les domaines VXLAN et non-VXLAN, connectant des périphériques sur différents réseaux.



Routeur entre domaines VXLAN

Avec un domaine de couche 2 étendu par VXLAN, une machine virtuelle peut pointer vers un ASA comme passerelle lorsque ASA ne se trouve pas sur le même rack, ou même lorsque l'ASA est éloigné sur le réseau de couche 3.





Consultez les remarques suivantes à propos de ce scénario :

1. Pour les paquets de la VM3 à la VM1, l'adresse MAC de destination est l'adresse MAC ASA, car l'ASA est la passerelle par défaut.
2. L'interface source de VTEP sur le serveur virtuel 2 reçoit les paquets de VM3, puis encapsule les paquets avec la balise VXLAN de VNI 3 et les envoie à l'ASA.
3. Lorsque l'ASA reçoit les paquets, il désencapsule les paquets pour obtenir les trames internes.
4. L'ASA utilise les cadres internes pour la recherche de routage, puis trouve que la destination est sur VNI 2. S'il n'a pas encore de mappage pour VM1, l'ASA envoie une diffusion ARP encapsulée sur l'adresse IP du groupe de multidiffusion sur VNI 2.

Remarque L'ASA doit utiliser la découverte d'homologues VTEP dynamique, car il a plusieurs homologues VTEP dans ce scénario.

5. L'ASA encapsule de nouveau les paquets avec la balise VXLAN pour VNI 2 et envoie les paquets au serveur virtuel 1. Avant l'encapsulation, l'ASA modifie l'adresse MAC de destination de la trame interne pour qu'elle corresponde à l'adresse MAC de VM1 (l'ARP encapsulé en multidiffusion peut être nécessaire pour que l'ASA apprenne l'adresse MAC de VM1).
6. Lorsque le serveur virtuel 1 reçoit les paquets VXLAN, il désencapsule les paquets et achemine les trames internes à la VM1.

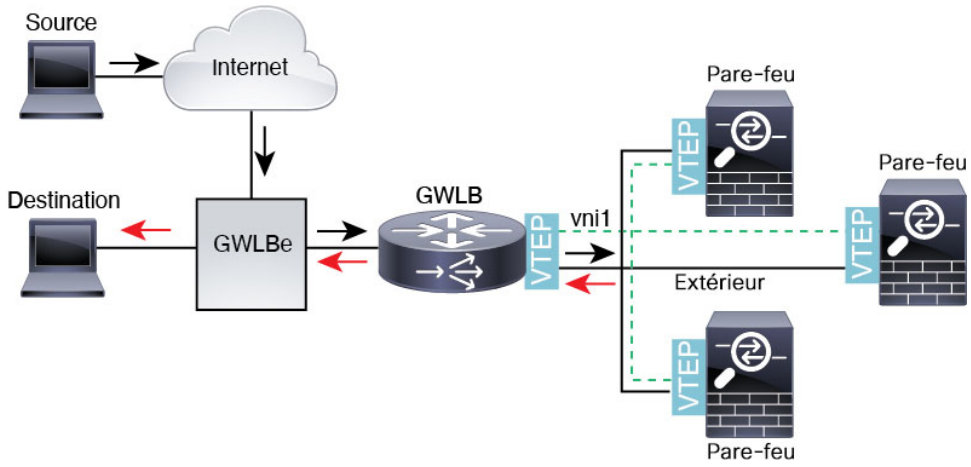
Équilibreur de charge de passerelle AWS et serveur mandataire à un seul volet de Geneve

Remarque Ce scénario est le seul actuellement pris en charge pour les interfaces de Geneve.

L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. Le ASA virtuel prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point terminal de l'équilibreur de charge de passerelle). La figure suivante montre le trafic acheminé

vers l'équilibreur de charge de passerelle à partir du point terminal de l'équilibreur de charge de passerelle. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs ASA virtuel, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle (trafic à demi-tour). L'équilibreur de charge de passerelle renvoie ensuite le trafic au point terminal de l'équilibreur de charge de passerelle et à la destination.

Illustration 63 : Serveur mandataire à un seul volet Geneve

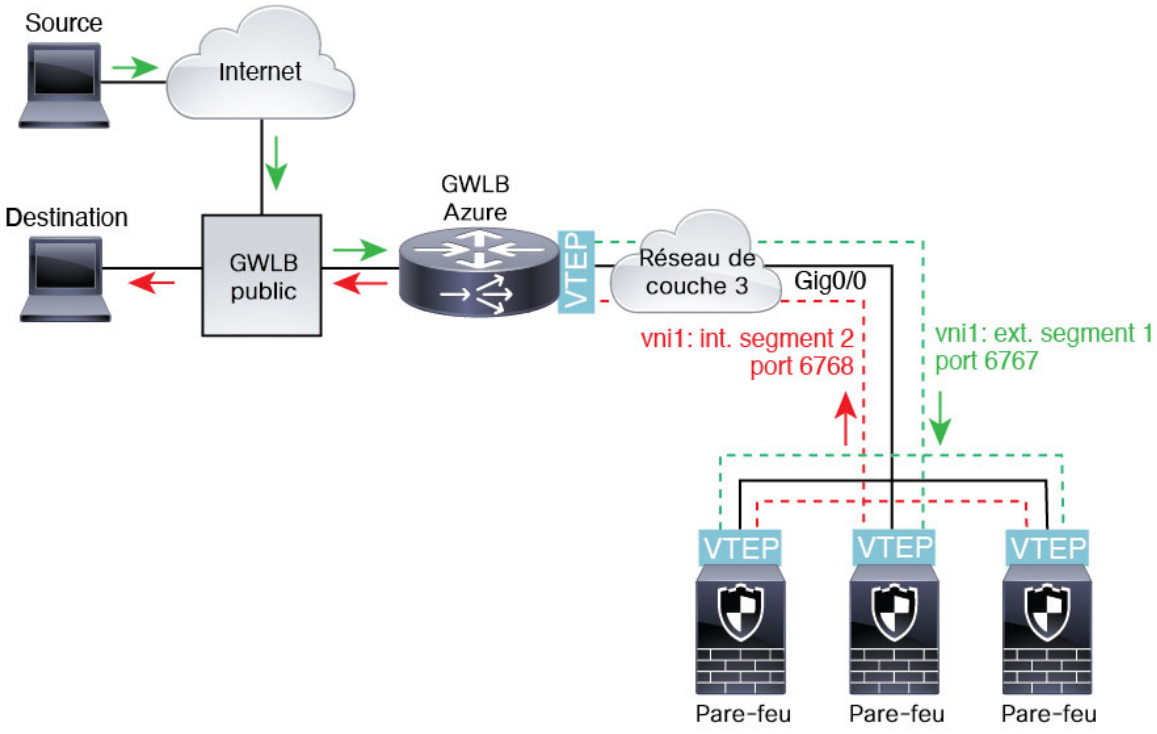


Équilibreur de charge de passerelle Azure et serveur mandataire jumelé

Dans une chaîne de service Azure, les ASA virtuelagissent comme une passerelle transparente qui peut intercepter les paquets entre Internet et le service client. Le ASA virtuel définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un serveur mandataire apparié.

La figure suivante montre le trafic transféré vers l'équilibreur de charge de passerelle Azure à partir de l'équilibreur de charge de passerelle publique sur le segment VXLAN externe. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs ASA virtuel, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle sur le segment VXLAN interne. L'équilibreur de charge de passerelle Azure renvoie ensuite le trafic vers l'équilibreur de charge de passerelle publique et vers la destination.

Illustration 64 : Équilibreur de charge de passerelle Azure avec mandataire jumelé



Exigences et conditions préalables pour les interfaces VXLAN

Exigences du modèle

- Les ports de commutation Firepower 1010 et les interfaces VLAN ne sont pas pris en charge en tant qu'interfaces VTEP.
- L'encapsulation Geneve est prise en charge pour les modèles suivants : ASAv30, ASAv50, ASAv100 sur Amazon Web Services (AWS)
- Le réseau VXLAN en mode proxy jumelé est pris en charge pour les modèles suivants :
  - ASA virtuel dans Azure

Lignes directrices pour les interfaces VXLAN

Mode pare-feu

- Les interfaces Geneve ne sont prises en charge qu'en mode de pare-feu routé.
- Les interfaces VXLAN mandataires jumelées ne sont prises en charge qu'en mode de pare-feu routé.

IPv6

- L'interface VNI prend en charge le trafic IPv4 et IPv6.
- L'adresse IP de l'interface source VTEP prend uniquement en charge IPv4.

Mise en grappe et mode de contexte multiple

- La mise en grappe d'ASA ne prend pas en charge VXLAN en mode d'interface individuelle, sauf pour la liaison de commande de grappe (ASA virtuel seulement). Seul le mode EtherChannel étendu prend en charge VXLAN.

  Une exception est faite pour l'ASA virtuel sur AWS, qui peut utiliser une interface Geneve supplémentaire à utiliser avec GWLB.
- Les interfaces Geneve ne sont prises en charge qu'en mode en mode de contexte unique. Elles ne sont pas prises en charge avec le mode de contexte multiple.

Routage

- Seul le routage statique ou le routage basé sur des politiques est pris en charge sur l'interface VNI; les protocoles de routage dynamique ne sont pas pris en charge.

VPN

Vous ne pouvez pas configurer l'interface source VTEP pour le VPN ou l'utiliser comme VTI.

MTU

- Encapsulation VXLAN : si la MTU de l'interface source est inférieure à 1 554 octets pour IPv4 ou à 1 574 octets pour IPv6 ou 1 574 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 54 octets. Cette MTU nécessite l'activation de la réservation de bâti grand format sur certains modèles; voir Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 678.
- Encapsulation Geneve : si la MTU de l'interface source est inférieure à 1 806 octets, l'ASA fait automatiquement passer la MTU à 1 806 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 306 octets. Cette MTU nécessite l'activation de la réservation de bâti grand format sur certains modèles; voir Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 678.

Paramètres par défaut des interfaces VXLAN

Les interfaces VNI sont activées par défaut.

Configurer les interfaces VXLAN

Pour configurer les interfaces VXLAN, procédez comme suit.

Remarque Vous pouvez configurer VXLAN ou Geneve (ASA virtuel uniquement). Pour les interfaces Geneve, consultez Configurer les interfaces Geneve, à la page 750.

Procédure

Étape 1 Configurer l'interface source VTEP, à la page 745.

Étape 2 Configurer l'interface VNI, à la page 747

Étape 3 (Facultatif) Modifier le port UDP VXLAN, à la page 750.

Étape 4 (Azure GWLB) Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle, à la page 753.

Configurer l'interface source VTEP

Vous pouvez configurer une interface source de VTEP par ASA ou par contexte de sécurité. Le VTEP est défini comme un terminal de virtualisation de réseau (NVE).

Avant de commencer

Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Saisissez la commande **changeto context** *name* pour remplacer le contexte que vous souhaitez configurer.

Procédure

Étape 1 (Mode transparent) Spécifiez que l'interface source est NVE uniquement :

interface *id*

nve-only

Exemple :

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

Ce paramètre vous permet de configurer une adresse IP pour l'interface. Cette commande est facultative pour le mode routé où ce paramètre limite le trafic à VXLAN et au trafic de gestion commun uniquement sur cette interface.

Étape 2 Configurez le nom de l'interface source et l'adresse IPv4 .

Exemple :

(Mode routé)

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

Exemple :

(Mode transparent)

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

Étape 3 Spécifiez l'instance NVE :

nve 1

Vous ne pouvez spécifier qu'une seule instance NVE, avec l'ID 1.

Exemple :

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)#
```

Étape 4 Spécifiez l'encapsulation VXLAN.

encapsulation vxlan

Exemple :

```
ciscoasa(cfg-nve)# encapsulation vxlan
```

Étape 5 Spécifiez le nom de l'interface source que vous avez configuré à l'étape 2 :

source-interface *interface-name*

Exemple :

```
ciscoasa(cfg-nve)# source-interface outside
```

Remarque
Si la MTU de l'interface VTEP est inférieure à 1 554 octets, l'ASA augmente automatiquement la MTU à 1 554 octets.

Étape 6 (Mode de contexte multiple; facultatif pour le mode unique) Spécifiez manuellement l'adresse IP VTEP de l'homologue :

peer ip *ip_address*

Exemple :

```
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

Si vous spécifiez l'adresse IP de l'homologue, vous ne pouvez pas utiliser la découverte de groupe de multidiffusion. La multidiffusion n'est pas prise en charge en mode de contexte multiple, la configuration manuelle est donc la seule option. Vous ne pouvez définir qu'un seul homologue pour le VTEP.

Étape 7 (Facultatif; mode unique seulement) Spécifiez un groupe de multidiffusion par défaut pour toutes les interfaces VNI associées :

default-mcast-group *mcast_ip*

Exemple :

```
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

Si vous ne configurez pas le groupe de multidiffusion par interface VNI, ce groupe est utilisé. Si vous configurez un groupe au niveau de l'interface VNI, ce groupe remplace ce paramètre.

Configurer l'interface VNI

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

Pour l'ASA virtuel dans Azure, vous pouvez configurer une interface VXLAN standard ou une interface VXLAN en mode de mandataire jumelé à utiliser avec la GWLB Azure.

Procédure

Étape 1 Créez l'interface VNI :

interface vni *vni_num*

Exemple :

```
ciscoasa(config)# interface vni 1
```

Définissez l'ID entre 1 et 10 000. Cet ID est uniquement un identifiant d'interface interne.

Étape 2 (VXLAN standard) Spécifiez l'ID de segment VXLAN :

segment-id *ID*

Exemple :

```
ciscoasa(config-if)# segment-id 1000
```

Définissez l'ID entre 1 et 16777215. L'ID de segment est utilisé pour le balisage VXLAN.

Étape 3 (Serveur mandataire VXLAN jumelé pour Azure GWLB) Activez le mode de mandataire jumelé et définissez les paramètres requis.

a) Activez le mode de mandataire jumelé.

proxy paired

Exemple :

```
ciscoasa(config-if)# proxy paired
```

b) Définissez le port interne.

internal-port *port_number*

Lorsque le paramètre *port_number* est compris entre 1024 et 65535.

Exemple :

```
ciscoasa(config-if)# internal-port 2000
```

c) Définissez l'ID de segment interne.

internal-segment-id *id_number*

Lorsque le paramètre *id_number* est compris entre 1 et 16777215.

Exemple :

```
ciscoasa(config-if)# internal-segment-id 101
```

d) Définissez le port externe.

external-port *port_number*

Lorsque le paramètre *port_number* est compris entre 1024 et 65535.

Exemple :

```
ciscoasa(config-if)# external-port 2001
```

e) Définissez l'ID de segment externe.

external-segment-id *id_number*

Lorsque le paramètre *id_number* est compris entre 1 et 16777215.

Exemple :

```
ciscoasa(config-if)# external-segment-id 102
```

f) Autorisez le trafic à entrer et à sortir de la même interface.

same-security-traffic permit intra-interface

Exemple :

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

Étape 4 (Obligatoire pour le mode transparent) Spécifiez le groupe de ponts auquel vous souhaitez associer cette interface :

bridge-group *number*

Exemple :

```
ciscoasa(config-if)# bridge-group 1
```

Consultez Configurer les interfaces de groupe de ponts, à la page 772 pour configurer l'interface BVI et associer des interfaces standard à ce groupe de ponts.

Étape 5 Associez cette interface à l'interface source VTEP :

vtep-nve 1

Étape 6 Nommez l'interface :

nameif *vni_interface_name*

Exemple :

```
ciscoasa(config-if)# nameif vxlan1000
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 7 (Mode routé) Attribuez une adresse IPv4 et/ou IPv6 :

ip address {*ip_address* [*mask*] [**standby** *ip_address*] | **dhcp** [**setroute**] | **pppoe** [**setroute**]}

ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-address*]}

Exemple :

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

Étape 8 Définissez le niveau de sécurité :

security-level *level*

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Où *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 9 (Mode unique) Définissez l'adresse du groupe de multidiffusion :

mcast-group *multicast_ip*

Exemple :

```
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Si vous ne définissez pas le groupe de multidiffusion pour l'interface VNI, le groupe par défaut de la configuration de l'interface source VTEP est utilisé, s'il est disponible. Si vous définissez manuellement une adresse IP homologue VTEP pour l'interface source de VTEP, vous ne pouvez pas spécifier de groupe de multidiffusion pour l'interface VNI. La multidiffusion n'est pas prise en charge en mode de contexte multiple.

(Facultatif) Modifier le port UDP VXLAN

Par défaut, l'interface source VTEP accepte le trafic VXLAN vers le port UDP 4789. Si votre réseau utilise un port non standard, vous pouvez le modifier.

Avant de commencer

Pour le mode de contexte multiple, effectuez cette tâche dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Définissez le port UDP VXLAN :

vxlan *port number*

Exemple :

```
ciscoasa(config)# vxlan port 5678
```

Configurer les interfaces Geneve

Pour configurer les interfaces de Geneve pour ASA virtuel, procédez comme suit.

Remarque Vous pouvez configurer VXLAN ou Geneve. Pour les interfaces VXLAN, consultez Configurer les interfaces VXLAN, à la page 745.

Procédure

Étape 1 Configurer l'interface source VTEP pour Geneve, à la page 751.

Étape 2 Configurer l'interface VNI pour Geneve, à la page 752

Étape 3 Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle, à la page 753.

Configurer l'interface source VTEP pour Geneve

Vous pouvez configurer une interface source de VTEP par ASA virtuel. Le VTEP est défini comme un point terminal de virtualisation du réseau (NVE).

Procédure

Étape 1 (Facultatif) Indiquez que l'interface source est NVE uniquement.

interface *id*

nve-only

Exemple :

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

Ce paramètre limite le trafic à VXLAN et au trafic de gestion commun uniquement sur cette interface.

Étape 2 Configurez le nom de l'interface source et l'adresse IPv4.

Exemple :

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

Étape 3 Spécifiez l'instance NVE :

nve 1

Vous ne pouvez spécifier qu'une seule instance NVE, avec l'ID 1.

Exemple :

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)#
```

Étape 4 Spécifiez l'encapsulation Geneve.

encapsulation geneve

Ne modifiez pas le port Geneve; AWS nécessite un port 6081.

Exemple :

```
ciscoasa(cfg-nve)# encapsulation geneve
```

Étape 5 Spécifiez le nom de l'interface source que vous avez configuré à l'étape 2 :

source-interface *interface-name*

Exemple :

```
ciscoasa(cfg-nve)# source-interface outside
```

Remarque
Si la MTU de l'interface source est inférieure à 1 806 octets, l'ASA augmente automatiquement la MTU à 1 806 octets.

Configurer l'interface VNI pour Geneve

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

Procédure

Étape 1 Créez l'interface VNI :

interface vni *vni_num*

Exemple :

```
ciscoasa(config)# interface vni 1
```

Définissez l'ID entre 1 et 10 000. Cet ID est uniquement un identifiant d'interface interne.

Étape 2 Associez cette interface à l'interface source VTEP :

vtep-nve 1

Étape 3 Nommez l'interface :

nameif *vni_interface_name*

Exemple :

```
ciscoasa(config-if)# nameif geneve1000
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 4 Attribuez une adresse IPv4 et/ou IPv6 :

ip address {*ip_address* [*mask*] [**standby** *ip_address*]}

ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-address*]}

Geneve ne prend en charge qu'une adresse IP statique.

Exemple :

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
```

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

Étape 5 Définissez le niveau de sécurité :

security-level *level*

Où *level* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Étape 6 Activez le serveur mandataire à un seul volet .

proxy single-arm

Exemple :

```
ciscoasa(config-if)# proxy single-arm
```

Étape 7 Autorisez le trafic à entrer et à sortir de la même interface.

same-security-traffic permit intra-interface

Exemple :

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle

L'équilibreur de charges de la passerelle AWS ou Azure nécessite des périphériques pour répondre correctement à une vérification de l'intégrité. L'équilibreur de charges de la passerelle AWS enverra uniquement le trafic vers des périphériques considérés comme intègres.

Vous devez configurer l'ASA virtuel pour répondre à une vérification de l'intégrité SSH, HTTP ou HTTPS.

Connexion SSH

Pour SSH, autorisez SSH à partir de l'équilibreur de charges de la passerelle. L'équilibreur de charges de la passerelle tentera d'établir une connexion à ASA virtuel, et l'invite de connexion de ASA virtuel est considérée comme une preuve de l'intégrité.

Remarque Une tentative de connexion SSH expirera après 1 minute. Vous devrez configurer un intervalle de vérification de l'intégrité plus long sur l'équilibreur de charges de la passerelle pour tenir compte de ce délai.

Exemple

```
! Allow SSH connections from GWLB network: 10.0.1.0/24
```

```
ssh 10.0.1.0 255.255.255.0 outside
```

Connexion Telnet

Pour Telnet, autorisez Telnet à partir de l'équilibreur de charges de la passerelle. L'équilibreur de charges de la passerelle tentera d'établir une connexion à ASA virtuel, et l'invite de connexion de ASA virtuel est considérée comme une preuve de l'intégrité.



Remarque Vous ne pouvez pas vous connecter via Telnet à l'interface du niveau de sécurité le plus bas, donc cette méthode peut ne pas être pratique.

Exemple

```
! Allow Telnet connections from GWLB network: 10.0.1.0/24
telnet 10.0.1.0 255.255.255.0 outside
```

Mandataire direct HTTP(S)

Vous pouvez configurer l'ASA pour demander à l'équilibreur de charges de la passerelle de vous connecter par HTTP(S).

Exemple

```
! Identify health probe HTTP traffic from GWLB nw 10.0.1.0/24 to ASAv interface 10.2.2.2
access-list gwlb extended permit tcp 10.0.1.0 255.255.255.0 host 10.2.2.2 eq www
! Enable HTTP authentication
aaa authentication http console LOCAL
! Require authentication for the health probe traffic
aaa authentication match gwlb outside LOCAL
! Use an HTTP login page on the ASA
aaa authentication listener http outside port www
```

Redirection HTTP(S) à l'aide de la NAT d'interface statique avec traduction de port

Vous pouvez configurer ASA virtuel pour rediriger les vérifications de l'intégrité vers un serveur HTTP(S) de métadonnées. Pour les vérifications de l'intégrité HTTP(S), le serveur HTTP(S) doit répondre à l'équilibreur de charges de la passerelle avec un code d'état compris entre 200 et 399. Étant donné que l'ASA virtuel a des limites sur le nombre de connexions de gestion simultanées, vous pouvez choisir de décharger le contrôle de l'intégrité sur un serveur externe.

La NAT d'interface statique avec traduction de port vous permet de rediriger une connexion vers un port (comme le port 80) vers une adresse IP différente. Par exemple, traduisez un paquet HTTP de l'équilbreur de charges de la passerele avec la destination de l'interface externe ASA virtuel de sorte qu'il semble provenir de l'interface externe ASA virtuel avec la destination du serveur HTTP. Le ASA virtuel transfère ensuite le paquet vers l'adresse de destination mappée. Le serveur HTTP répond à l'interface externe ASA virtuel, puis ASA virtuel renvoie la réponse à l'équilibreur de charges de la passerelle. Vous avez besoin d'un critère d'accès qui autorise le trafic de l'équilibreur de charges de la passerelle vers le serveur HTTP.

Exemple

```
! Permit HTTP traffic from GWLB nw 10.0.1.0/24 to HTTP server 10.2.2.3
```

```
access-list gwlb-health extended permit tcp 10.0.1.0 255.255.255.0 host 10.2.2.3 eq www
access-group gwlb-health in interface outside

! Create network objects
object network gwlb-subnet
 subnet 10.0.1.0 255.255.255.0
object-group network gwlb
    network-object object gwlb-subnet
object-group network http-server
    network-object host 10.2.2.3
object service http80
    service tcp destination eq www

! For HTTP, translate src GWLB IP to outside IP; translate dest of outside IP to HTTP Server
 IP
nat (outside,outside) source static gwlb interface destination static interface http-server
 service http80 http80
```

Supervision des interfaces VXLAN

Consultez les commandes suivantes pour superviser les interfaces VTEP et VNI.

- **show nve** [*id*] [**summary**]

  Cette commande affiche les paramètres, l'état et les statistiques d'une interface NVE, l'état de son interface de transport (interface source), l'adresse IP de l'interface de transport, les VNI qui utilisent ce NVE comme le VXLAN VTEP et les adresses IP VTEP des pairs associées à cette interface NVE. Avec l'option **summary**, cette commande affiche uniquement l'état de l'interface NVE, le nombre de VNI derrière l'interface NVE et le nombre de VTEP découverts.

  Consultez la sortie suivante pour la commande **show nve 1** :

```
ciscoasa# show nve 1
ciscoasa(config-if)# show nve
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 15.1.2.3
Number of VNIs attached to nve 1: 2
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

  Consultez la sortie suivante pour la commande **show nve 1 summary** :

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Default multicast group: 239.1.2.3
```

```
Number of VNIs attached to nve 1: 2
```

- **show interface vni** *id* [**summary**]

  Cette commande affiche les paramètres, l'état et les statistiques d'une interface VNI, l'état de son interface pontée (si configurée) et l'interface NVE à laquelle elle est associée. L'option **summary** affiche uniquement les paramètres d'interface VNI.

  Consultez la sortie suivante pour la commande **show interface vni 1** :

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

  Consultez la sortie suivante pour la commande **show interface vni 1 summary** :

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

- **show vni vlan-mapping**

  Cette commande affiche le mappage entre les ID de segment VNI et les interfaces VLAN ou les interfaces physiques. Cette commande n'est valide qu'en mode de pare-feu transparent, car en mode routé, le mappage entre les VXLAN et les VLAN peut inclure trop de valeurs à afficher.

  Consultez la sortie suivante pour la commande **show vni vlan-mapping** :

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3, interface:
 'g112', vlan 4
```

- **show arp vtep-mapping**

Cette commande affiche les adresses MAC mises en mémoire cache sur l'interface VNI pour les adresses IP situées dans le domaine de segment distant et les adresses IP VTEP distantes.

Consultez la sortie suivante pour la commande **show arp vtep-mapping** :

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

- **show mac-address-table vtep-mapping**

  Cette commande affiche le tableau de transfert de couche 2 (table d'adresses MAC) sur l'interface VNI avec les adresses IP VTEP distantes.

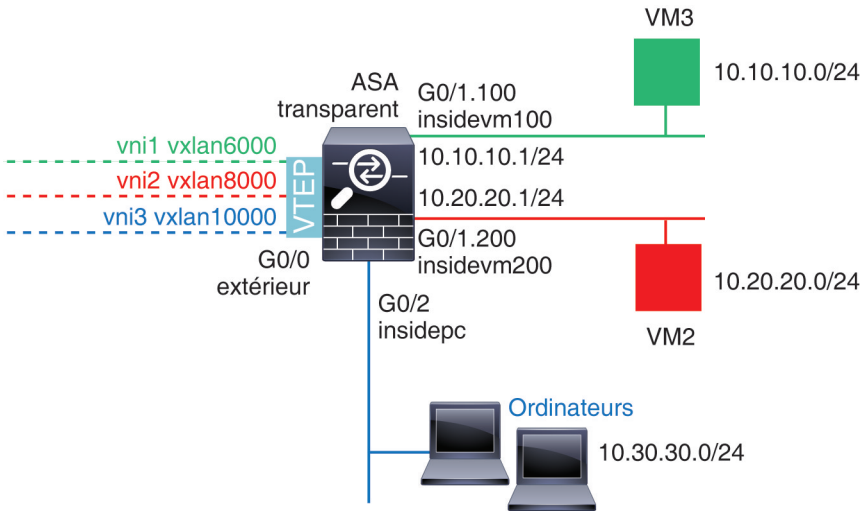
  Consultez la sortie suivante pour la commande **show mac-address-table vtep-mapping** :

```
ciscoasa# show mac-address-table vtep-mapping
interface                  mac  address       type      Age(min)    bridge-group     VTEP
------------------------------------------------------------------------------------------
vni-outside               00ff.9200.0000      dynamic      5          1          10.9.1.3
vni-inside                 0041.9f00.0000      dynamic      5          1        10.9.1.3
```

Exemples d'interfaces VXLAN

Consultez les exemples de configuration suivants pour VXLAN.

Exemple de passerelle VXLAN transparente



Consultez la description suivante de cet exemple :

- L'interface externe sur GigabitEthernet 0/0 est utilisée comme interface source VTEP et est connectée au réseau de couche 3.

- La sous-interface VLAN insidevm100 sur GigabitEthernet 0/1.100 est connectée au réseau 10.10.10.0/24, sur lequel réside VM3. Lorsque VM3 communique avec VM1 (non affiché; les deux ont des adresses IP 10.10.10.0/24), l'ASA utilise la balise VXLAN 6000.
- La sous-interface VLAN insidevm200 sur GigabitEthernet 0/1.200 est connectée au réseau 10.20.20.0/24, sur lequel réside VM2. Lorsque VM2 communique avec VM4 (non affiché; les deux ont des adresses IP 10.20.20.0/24), l'ASA utilise la balise VXLAN 8000.
- L'interface insidepc de GigabitEthernet 0/2 est connectée au réseau 10.30.30.0/24 sur lequel se trouvent quelques ordinateurs. Lorsque ces ordinateurs communiquent avec des VM/PC (non affichés) derrière un VTEP distant qui appartient au même réseau (tous ont des adresses IP 10.30.30.0/24), l'ASA utilise la balise VXLAN 10000.

Configuration ASA

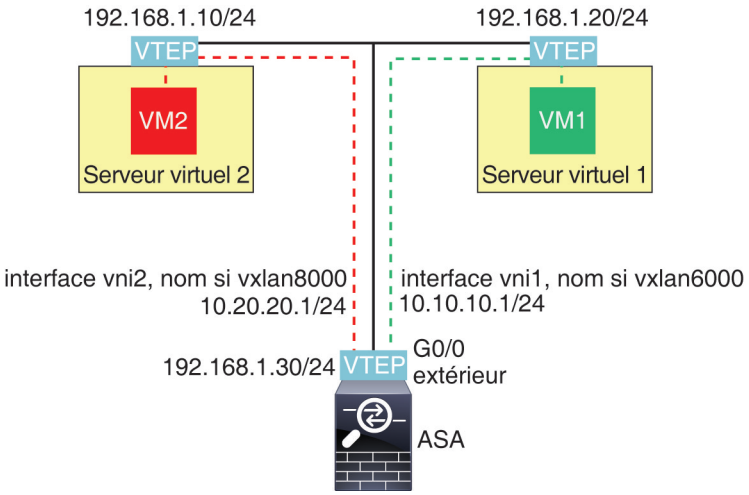
```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
```

```
  bridge-group 2
!
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
  ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
  ip address 10.30.30.1 255.255.255.0
```

Notes

- Pour les interfaces VNI vni1 et vni2, la balise VLAN interne est supprimée pendant l'encapsulation.
- Les interfaces VNI vni2 et vni3 partagent la même adresse IP de multidiffusion pour l'ARP encapsulé sur la multidiffusion. Ce partage est autorisé.
- L'ASA relie le trafic VXLAN vers des interfaces non prises en charge par VXLAN en fonction des BVI et des configurations de groupes de ponts ci-dessus. Pour chacun des segments de réseau étendus de couche 2 (10.10.10.0/24, 10.20.20.0/24 et 10.30.30.0/24), l'ASA sert de pont.
- Il est autorisé d'avoir plusieurs VNI ou plusieurs interfaces standard (VLAN ou simplement interface physique) dans un groupe de ponts. Le transfert ou l'association entre l'ID de segment VXLAN et l'ID de VLAN (ou une interface physique) est décidé par l'adresse MAC de destination et l'interface qui se connecte à la destination.
- L'interface source VTEP est une interface de couche 3 en mode de pare-feu transparent, indiquée par **nve-only** dans la configuration de l'interface. L'interface source VTEP n'est pas une interface BVI ni une interface de gestion, mais elle a une adresse IP et utilise la table de routage.

Exemple de routage VXLAN



Consultez la description suivante de cet exemple :

- VM1 (10.10.10.10) est hébergé sur le serveur virtuel 1 et VM2 (10.20.20.20) est hébergé sur le serveur virtuel 2.
- La passerelle par défaut pour VM1 est l'ASA, qui ne se trouve pas dans le même module que le serveur virtuel 1, mais VM1 ne le sait pas. VM1 sait uniquement que l'adresse IP de sa passerelle par défaut est 10.10.10.1. De même, VM2 sait uniquement que l'adresse IP de sa passerelle par défaut est 10.20.20.1.
- Les hyperviseurs pris en charge par le VTEP sur les serveurs virtuels 1 et 2 peuvent communiquer avec l'ASA sur le même sous-réseau ou par l'intermédiaire d'un réseau de couche 3 (non illustré; dans ce cas, l'ASA et les liaisons ascendantes des serveurs virtuels ont des adresses réseau différentes).
- Le paquet de VM1 sera encapsulé par le VTEP de son hyperviseur et envoyé à sa passerelle par défaut sur la tunnellisation VXLAN.
- Lorsque VM1 envoie un paquet à VM2, le paquet sera envoyé par la passerelle par défaut 10.10.10.1 de son point de vue. Le serveur virtuel 1 sait que la passerelle 10.10.10.1 n'est pas locale; par conséquent, le VTEP encapsule le paquet sur VXLAN et l'envoie au VTEP de l'ASA.
- Sur l'ASA, le paquet est désencapsulé. L'ID de segment VXLAN est appris lors de la désencapsulation. L'ASA réinjecte ensuite le cadre interne dans l'interface VNI (vni1) correspondante en fonction de l'ID de segment VXLAN. L'ASA effectue ensuite une recherche de route et envoie le paquet interne par une autre interface VNI, vni2. Tous les paquets sortants par vni2 sont encapsulés avec le segment VXLAN 8000 et envoyés par le VTEP à l'extérieur.
- Finalement, le paquet encapsulé est reçu par le VTEP du serveur virtuel 2, qui le désencapsule et le transfère à VM2.

Configuration ASA

```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
  ip address 10.10.10.1 255.255.255.0
!
```

Historique des interfaces VXLAN

Tableau 30 : Historique des interfaces VXLAN

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Proxy jumelé VXLAN pour l'ASA virtuel pour l'équilibreur de charges de la passerelle Azure.	9.19(1)	Vous pouvez configurer une interface VXLAN en mode proxy apparié pour l'ASA virtuel dans Azure afin de l'utiliser avec l'équilibreur de charges de la passerelle Azure (GWLB). L'ASA virtuel définit une interface externe et une interface interne sur un seul NIC en utilisant des segments VXLAN dans un serveur mandataire jumelé. Commandes nouvelles/modifiées : **port externe, segment-id externe, port interne, segment-id interne, proxy paired**
Prise en charge de Geneve pour le ASA virtuel sur AWS pour l'équilibreur de charges de la passerelle AWS	9.17(1)	La prise en charge de l'encapsulation Geneve a été ajoutée pour l'ASAv30, ASAv50 et ASAv100 afin de prendre en charge le serveur mandataire à un seul volet pour l'équilibreur de charges de passerelle AWS. Commandes nouvelles ou modifiées : **debug geneve**, **debug nve**, **debug vxlan**, **encapsulation**, **packet-tracer geneve**, **proxy single-arm**, **show asp drop**, **show capture**, **show interface**, **show nve**
Prise en charge de VXLAN	9.4(1)	La prise en charge de VXLAN a été ajoutée, y compris la prise en charge du terminal de tunnel VXLAN (VTEP). Vous pouvez définir une interface source VTEP par ASA ou contexte de sécurité. Nous avons introduit les commandes suivantes : **debug vxlan**, **default-mcast-group**, **encapsulation vxlan**, **inspect vxlan**, **interface vni**, **mcast-group**, **nve**, **nve-only**, **peer ip**, **segment-id**, **show arp vtep-mapping**, **show interface vni**, **show mac-address-table vtep-mapping**, **show nve**, **show vni vlan-mapping**, **source-interface**, **vtep-nve**, **vxlan port**



CHAPITRE 20

Interfaces en mode routage et en mode transparent

Ce chapitre comprend des tâches pour terminer la configuration de l'interface pour tous les modèles en mode de pare-feu routé ou transparent.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Saisissez la commande **changeto context** *name* pour remplacer le contexte que vous souhaitez configurer.

- À propos des interfaces en mode routage et en mode transparent, à la page 763
- Directives et limites pour les interfaces en mode routé et en mode transparent, à la page 765
- Configurer les interfaces en mode routé, à la page 767
- Configurer les interfaces de groupe de ponts, à la page 772
- Configuration de l'adressage IPv6, à la page 778
- Supervision des interfaces en mode routé et en mode transparent, à la page 790
- Exemples d'interfaces en mode routé et en mode transparent, à la page 796
- Historique des interfaces en mode routé et en mode transparent, à la page 799

À propos des interfaces en mode routage et en mode transparent

L'ASA prend en charge deux types d'interfaces : routées et pontées.

Chaque interface routée de couche 3 nécessite une adresse IP sur un sous-réseau unique.

Les interfaces pontées appartiennent à un groupe de ponts et toutes les interfaces se trouvent sur le même réseau. Le groupe de ponts est représenté par une interface virtuelle de pont (BVI) qui a une adresse IP sur le réseau de ponts. Le mode routé prend en charge les interfaces routées et pontées, et vous pouvez effectuer le routage entre des interfaces routées et des BVI. Le mode de pare-feu transparent ne prend en charge que les interfaces de groupe de ponts et BVI.

Niveaux de sécurité

Chaque interface doit avoir un niveau de sécurité de 0 (le plus bas) à 100 (le plus élevé), y compris les interfaces membres d'un groupe de ponts. Par exemple, vous devez affecter votre réseau le plus sécurisé, comme le réseau d'hôte interne, au niveau 100. Le réseau externe connecté à Internet peut quant à lui être attribué au

niveau 0. D'autres réseaux, tels que les DMZ, peuvent être entre les deux. Vous pouvez attribuer des interfaces au même niveau de sécurité.

L'attribution d'un niveau de sécurité à une BVI dépend du mode de pare-feu. En mode transparent, l'interface BVI n'a pas de niveau de sécurité, car elle ne participe pas au routage entre les interfaces. En mode routé, les interfaces BVI ont un niveau de sécurité si vous choisissez d'effectuer le routage entre les BVI et d'autres interfaces. Pour le mode routé, le niveau de sécurité d'une interface membre d'un groupe de ponts s'applique uniquement à la communication au sein du groupe de ponts. De même, le niveau de sécurité BVI s'applique uniquement à la communication inter-BVI/interface de couche 3.

Le niveau contrôle le comportement suivant :

- Accès au réseau : par défaut, il existe une autorisation implicite d'une interface de sécurité supérieure vers une interface de sécurité inférieure (sortante). Les hôtes de l'interface de sécurité supérieure peuvent accéder à n'importe quel hôte sur une interface de sécurité inférieure. Vous pouvez limiter l'accès en appliquant une ACL à l'interface.

  Si vous activez la communication pour des interfaces de même sécurité, il existe une autorisation implicite pour que les interfaces accèdent à d'autres interfaces sur le même niveau de sécurité ou un niveau de sécurité inférieur.

- Moteurs d'inspection : certains moteurs d'inspection d'applications dépendent du niveau de sécurité. Pour les interfaces de même sécurité, les moteurs d'inspection s'appliquent au trafic dans l'une ou l'autre direction.
  - Plateforme d'inspection NetBIOS : s'applique uniquement aux connexions sortantes.
  - Plateforme d'inspection SQL*Net : si une connexion de contrôle pour le port SQL*Net (anciennement OraServ) existe entre une paire d'hôtes, seule une connexion de données entrante est autorisée par l'ASA.

Double pile IP (IPv4 et IPv6)

L'ASA prend en charge les adresses IPv6 et IPv4 sur une interface. Assurez-vous de configurer une voie de routage par défaut pour IPv4 et IPv6.

Masque de sous-réseau 31 bits

Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, le lien de basculement entre 2 ASA ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog.

Sous-réseau 31 bits et mise en grappe

Vous pouvez utiliser un masque de sous-réseau de 31 bits de grappe en mode de mise en grappe étendue, à l'exclusion de l'interface de gestion et de la liaison de commande de grappe.

Vous ne pouvez pas utiliser un masque de sous-réseau de 31 bits en mode de mise en grappe individuelle sur une interface.

Sous-réseau 31 bits et basculement

Pour le basculement, lorsque vous utilisez un sous-réseau de 31 bits pour l'adresse IP d'interface ASA, vous ne pouvez pas configurer d'adresse IP de secours pour l'interface, car il n'y a pas assez d'adresses. Normalement, une interface de basculement doit avoir une adresse IP de secours pour que l'unité active puisse effectuer des tests d'interface pour s'assurer de l'intégrité de l'interface de secours. Sans adresse IP de secours, ASA ne peut effectuer aucun test de réseau. seul l'état du lien peut être suivi.

Pour le basculement et le lien à état séparé facultatif, qui sont des connexions point à point, vous pouvez également utiliser un sous-réseau de 31 bits.

Gestion et sous-réseau 31 bits

Si vous avez une station de gestion directement connectée, vous pouvez utiliser une connexion point à point pour SSH ou HTTP sur ASA, ou pour SNMP ou Syslog sur le poste de gestion.

Fonctionnalités 31 bits non prises en charge

Les fonctionnalités suivantes ne prennent pas en charge le sous-réseau de 31 bits :

- Interfaces BVI pour les groupes de ponts : le groupe de ponts nécessite au moins 3 adresses d'hôte : les BVI et deux hôtes connectés à deux interfaces membres du groupe de ponts. vous devez utiliser un sous-réseau /29 ou moins.
- Routage multidiffusion

Directives et limites pour les interfaces en mode routé et en mode transparent

Mode contextuel

- En mode de contexte multiple, vous pouvez seulement configurer les interfaces de contexte que vous avez déjà affectées au contexte dans la configuration système en fonction de Configurer plusieurs contextes, à la page 239.
- PPPoE n'est pas pris en charge en mode de contexte multiple.
- Pour le mode à contextes multiples en mode transparent, chaque contexte doit utiliser des interfaces différentes; vous ne pouvez pas partager une interface entre contextes.
- Pour le mode à contexte multiple en mode transparent, chaque contexte utilise généralement un sous-réseau différent. Vous pouvez utiliser des sous-réseaux qui se chevauchent, mais la topologie de votre réseau nécessite une configuration de routeur et de NAT pour que cela soit possible du point de vue du routage.
- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode de contexte multiple.
- En mode de pare-feu routé, les interfaces de groupes de ponts ne sont pas prises en charge dans le mode de contexte multiple.

Failover (basculement), mise en grappe

- Ne configurez pas les liens de basculement selon les procédures de ce chapitre. Consultez le chapitre Failover (basculement) pour plus de renseignements.
- Pour les interfaces de grappe, consultez le chapitre sur la mise en grappe pour connaître les exigences.
- Lorsque vous utilisez Failover (basculement), vous devez définir l'adresse IP et l'adresse de secours pour les interfaces de données manuellement. DHCP et PPPoE ne sont pas pris en charge.

IPv6

- IPv6 est pris en charge sur toutes les interfaces.
- Vous ne pouvez que configurer les adresses IPv6 manuellement en mode transparent.
- L'ASA ne prend pas en charge les adresses anycast IPv6.
- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode à contexte multiple, le mode transparent, la mise en grappe ou Failover (basculement).

Directives sur les modèles

- Pour l’ASAv50, les groupes de ponts ne sont pas pris en charge en mode transparent ou routé.
- Pour les périphériques Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.

Directives relatives au mode transparent et au groupe de ponts

- Vous pouvez créer jusqu’à 250 groupes de ponts, avec interfaces par groupe de ponts.
- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- L'ASA ne prend pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l’adresse IP BVI est pris en charge.
- Une adresse IP pour les BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par ASA. Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L’adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d’hôte (255.255.255.255).
- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- Pour l’ASAv50 sur VMware avec des interfaces ixgbevf pontées, le mode transparent n’est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Dans le cas du Firepower 1010, il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.
- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.

- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la ASA comme passerelle par défaut.
- En mode transparent, la voie de routage *par défaut*, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.
- Le protocole PPPoE n'est pas pris en charge sur l'interface Management (gestion).
- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par ASA et VNI ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de ASA lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de l'ASA exécutant BFD, alors l'ASA abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

Niveau de sécurité par défaut

Le niveau de sécurité par défaut est 0. Si vous nommez une interface « intérieur » et que vous ne définissez pas explicitement le niveau de sécurité, l'ASA le définit à 100.

Remarque Si vous modifiez le niveau de sécurité d'une interface et que vous ne souhaitez pas attendre que les connexions existantes expirent avant d'utiliser les nouveaux renseignements sur la sécurité, vous pouvez effacer les connexions à l'aide de la commande **clear conn**.

Directives et exigences supplémentaires

- Le ASA ne prend en charge qu'un seul en-tête 802.1Q par paquet et ne prend pas en charge plusieurs en-têtes (appelé prise en charge Q-in-Q).
- Des problèmes d'interface, tels que de fréquents changements d'état haut/bas, peuvent empêcher la minuterie de connexion flottante de s'appliquer correctement aux connexions passant par l'interface. Si vous avez des problèmes avec l'état d'une interface, pensez à effacer toutes les connexions une fois que l'état est stabilisé afin de supprimer les connexions non valides.

Configurer les interfaces en mode routé

Pour configurer les interfaces en mode routé, procédez comme suit.

Configurer les paramètres généraux de l'interface en mode routé

Cette procédure décrit comment définir le nom, le niveau de sécurité, l'adresse IPv4 et d'autres options.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *ID*

Exemple :

```
ciscoasa(config)# interface gigabithethernet 0/0
```

L'ID d'interface peut être :

- **canal de port**
- *physical*– Par exemple, **ethernet**, **gigabitethernet**, **10 gigabitethernet**, **gestion**. Reportez-vous au guide d'installation du matériel correspondant à votre modèle pour connaître les noms d'interface.
- *physical***.***subinterface*– Par exemple, **gigabitEthernet0/0.100**.
- **vni**
- **vlan**
- **loop back** (bouclage)
- *mapped_name*—Pour le mode de contexte multiple.

Remarque
Pour le Firepower 1010, vous ne pouvez pas configurer de ports de commutation en tant qu'interfaces en mode routé.

Étape 2 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif inside
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 3 Définissez l'adresse IP à l'aide de l'une des méthodes suivantes.

Pour le basculement et la mise en grappe, ainsi que pour les interfaces de boucle avec retour, vous devez définir l'adresse IP manuellement; les protocoles DHCP et PPPoE ne sont pas pris en charge.

- Définissez l'adresse IP manuellement :

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  L'argument *ip_address* en veille est utilisé pour le basculement. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

  Les arguments *ip_address* et *mask* définissent l'adresse IP de l'interface et le filtre d'adresse locale. Pour les connexions point à point, vous pouvez spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. Vous ne pouvez pas définir l'adresse IP de secours dans ce cas.

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.0 255.255.255.254
  ```

- Obtenez une adresse IP à partir d'un serveur DHCP :

  ip address dhcp [**setroute**]

  Exemple :

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  Le mot clé **setroute** permet à l'ASA d'utiliser la route par défaut fournie par le serveur DHCP.

  Saisissez à nouveau cette commande pour réinitialiser le bail locatif DHCP et demander un nouveau bail locatif.

  Remarque
  Si vous n'activez pas l'interface à l'aide de la commande **no shutdown** avant de saisir la commande **ip address dhcp**, certaines demandes DHCP pourraient ne pas être envoyées.

- Obtenez une adresse IP à partir d'un serveur PPPoE :

  ip address pppoe [**setroute**]

  Exemple :

  ```
  ciscoasa(config-if)# ip address pppoe setroute
  ```

  Vous pouvez également activer PPPoE en saisissant manuellement l'adresse IP :

  ip address *ip_address mask* **pppoe**

  Exemple :

```
ciscoasa(config-if)# ip address 10.1.1.78 255.255.255.0 pppoe
```

L'option **setroute** définit les routes par défaut lorsque le client PPPoE n'a pas encore établi de connexion. Lorsque vous utilisez l'option **setroute**, vous ne pouvez pas avoir de route définie de manière statique dans la configuration.

Remarque
Si le protocole PPPoE est activé sur deux interfaces (comme une interface principale et une interface de secours) et que vous ne configurez pas la prise en charge du double FAI, l'ASA ne pourra envoyer le trafic que par la première interface pour acquérir une adresse IP.

Étape 4 Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Le paramètre *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Remarque
Pour les interfaces de boucle avec retour, vous ne définissez pas de niveau de sécurité, car l'interface n'est prise en charge que pour le trafic vers/depuis le périphérique.

Étape 5 (Facultatif) Définissez une interface en mode gestion uniquement afin qu'elle ne transmette pas de trafic :

management-only

Par défaut, les interfaces de gestion sont configurées en tant que gestion uniquement.

Remarque
Pour les interfaces de boucle avec retour, vous ne définissez pas le mode de gestion, car l'interface n'est prise en charge que pour le trafic vers/depuis le périphérique.

Exemples

L'exemple suivant configure les paramètres pour le VLAN 101 :

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

L'exemple suivant configure les paramètres en mode de contexte multiple pour la configuration de contexte. L'ID d'interface est un nom mappé.

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
```

```
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

Sujets connexes

Configuration de l'adressage IPv6, à la page 778
Activer l'interface physique et configurer les paramètres Ethernet, à la page 675
Configurer le protocole PPPoE, à la page 771

Configurer le protocole PPPoE

Si l'interface est connectée à une liaison ADSL, à un modem câble ou à une autre connexion à votre FAI et que ce dernier utilise PPPoE pour vous fournir votre adresse IP, configurez les paramètres suivants.

Procédure

Étape 1 Définissez le nom du groupe de réseaux privés virtuels à accès commuté (Virtual Private Dialup Network ou VPDN) de votre choix pour représenter cette connexion :

vpdn group *group_name* **request dialout pppoe**

Exemple :

```
ciscoasa(config)# vpdn group pppoe-sbc request dialout pppoe
```

Étape 2 Si votre FAI requiert une authentification, sélectionnez un protocole d'authentification :

vpdn group *group_name* **ppp authentication** {**chap** | **mschap** | **pap**}

Exemple :

```
ciscoasa(config)# vpdn group pppoe-sbc ppp authentication chap
```

Saisissez le mot clé approprié pour le type d'authentification utilisé par votre FAI.

Lors de l'utilisation de CHAP ou de MS-CHAP, le nom d'utilisateur peut être appelé nom du système distant, tandis que le mot de passe peut être appelé secret CHAP.

Étape 3 Associez le nom d'utilisateur attribué par votre FAI au groupe VPDN :

vpdn group *group_name* **localname** *username*

Exemple :

```
ciscoasa(config)# vpdn group pppoe-sbc localname johncrichton
```

Étape 4 Créez une paire de nom d'utilisateur et de mot de passe pour la connexion PPPoE :

vpdn username *username* **password** *password* [**store-local**]

Exemple :

```
ciscoasa(config)# vpdn username johncrichton password moya
```

L'option **store-local** stocke le nom d'utilisateur et le mot de passe dans un emplacement spécial de la NVRAM sur l'ASA. Si un Auto Update Server envoie une commande **clear config** à l'ASA et que la connexion est interrompue, l'ASA peut lire le nom d'utilisateur et le mot de passe de NVRAM et s'authentifier de nouveau auprès du concentrateur d'accès.

Configurer les interfaces de groupe de ponts

Un groupe de ponts est un groupe d'interfaces que ASA relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Pour en savoir plus sur les groupes de ponts, consultez À propos des groupes de ponts, à la page 201.

Pour configurer des groupes de ponts et les interfaces associées, procédez comme suit.

Configurer la BVI (Bridge Virtual Interface)

Chaque groupe de ponts nécessite un BVI pour lequel vous configurez une adresse IP. L'ASA utilise cette adresse IP comme adresse source pour les paquets provenant du groupe de ponts. L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Pour le trafic IPv4, l'adresse IP BVI est requise pour laisser passer le trafic. Pour le trafic IPv6, vous devez, au minimum, configurer les adresses de lien locales pour laisser passer le trafic, mais une adresse de gestion globale est recommandée pour les fonctionnalités complètes, y compris la gestion à distance et d'autres opérations de gestion.

Pour le mode routé, si vous fournissez un nom pour les BVI, alors les BVI participent au routage. Sans nom, le groupe de ponts reste isolé comme en mode transparent de pare-feu.

Certains modèles incluent un groupe de ponts et une BVI dans la configuration par défaut. Vous pouvez créer des groupes de ponts et des BVI supplémentaires et réaffecter des interfaces membres entre les groupes.

Remarque Pour une interface de gestion distincte en mode transparent (pour les modèles pris en charge), un groupe de ponts non configurables (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.

Procédure

Étape 1 Créez une BVI :

interface bvi *bridge_group_number*

Exemple :

```
ciscoasa(config)# interface bvi 2
```

Le *bridge_group_number* est un nombre entier compris entre 1 et 250. Vous attribuerez ultérieurement des interfaces physiques à ce numéro de groupe de ponts.

Étape 2 (Mode transparent) Spécifiez l'adresse IP de la BVI :

ip address *ip_address* [*mask*] [**standby** *ip_address*]

Exemple :

```
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

N'affectez pas d'adresse hôte (/32 ou 255.255.255.255) au BVI. De plus, n'utilisez pas d'autres sous-réseaux contenant moins de 3 adresses d'hôte (une pour le routeur en amont, le routeur en aval et la BVI), comme un sous-réseau /30 (255.255.255.252). L'ASA abandonne tous les paquets ARP en provenance ou à destination de la première et de la dernière adresse d'un sous-réseau. Par conséquent, si vous utilisez un sous-réseau /30 et que vous affectez une adresse réservée de ce sous-réseau au routeur en amont, l'ASA abandonne la demande ARP du routeur en aval au routeur en amont.

Le mot clé **standby** et l'adresse sont utilisés pour le basculement.

Étape 3 (Mode routé) Définissez l'adresse IP à l'aide de l'une des méthodes suivantes.

Pour le basculement et la mise en grappe, vous devez définir l'adresse IP manuellement; le protocole DHCP n'est pas pris en charge.

- Définissez l'adresse IP manuellement :

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  L'argument *ip_address* en veille est utilisé pour le basculement.

  Les arguments *ip_address* et *mask* définissent l'adresse IP de l'interface et le filtre d'adresse locale.

- Obtenez une adresse IP à partir d'un serveur DHCP :

  ip address dhcp [**setroute**]

  Exemple :

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  Le mot clé **setroute** permet à l'ASA d'utiliser la route par défaut fournie par le serveur DHCP.

  Saisissez à nouveau cette commande pour réinitialiser le bail locatif DHCP et demander un nouveau bail locatif.

  Si vous n'activez pas l'interface à l'aide de la commande no shutdown avant de saisir la commande **ip address dhcp**, certaines demandes DHCP pourraient ne pas être envoyées.

Étape 4 (Mode routé) Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif inside
```

Vous devez nommer le BVI si vous souhaitez acheminer le trafic extérieur aux membres du groupe de pont, par exemple vers l'interface externe ou vers les membres d'autres groupes de pont. Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 5 (Mode routé) Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Le paramètre *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Exemple

L'exemple suivant définit l'adresse BVI 2 et l'adresse de veille :

```
ciscoasa(config)# interface bvi 2
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

Configurer les paramètres généraux de l'interface de membre du groupe de ponts

Cette procédure décrit comment définir le nom, le niveau de sécurité et le groupe de ponts pour chaque interface membre du groupe de ponts.

Avant de commencer

- Un même groupe de ponts peut inclure différents types d'interfaces : des interfaces physiques, des sous-interfaces VLAN, des interfaces VNI et des EtherChannels. Le protocole PPPoE n'est pas pris en charge sur l'interface de gestion. En mode routé, les EtherChannels et les VNI ne sont pas pris en charge.
- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.
- Pour le mode transparent, n'utilisez pas cette procédure pour les interfaces de gestion; consultez Configurer une interface de gestion pour le mode transparent, à la page 776 pour configurer l'interface de gestion.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *id*

Exemple :

```
ciscoasa(config)# interface gigabithethernet 0/0
```

L'ID d'interface peut être :

- **canal de port**
- *physical*– Par exemple, **ethernet**, **gigabitethernet**, **10 gigabitethernet**. Les interfaces de gestion ne sont pas prises en charge. Reportez-vous au guide d'installation du matériel correspondant à votre modèle pour connaître les noms d'interface.
- *Physical_or_port-canal***.***subinterface*– Par exemple, **gigabitethernet0/0.100** ou **port-channel1.100**.
- **vni**
- **vlan**
- *mapped_name*—Pour le mode de contexte multiple.

Remarque
Pour Firepower 1010, vous ne pouvez pas configurer de ports de commutation en tant que membres d'un groupe de ponts.

Vous ne pouvez pas mélanger des interfaces VLAN logiques et des interfaces de routeur physiques dans le même groupe de ponts.

Remarque
En mode routé, les interfaces **port-channel** et **vni** ne sont pas prises en charge en tant que membres de groupes de ponts.

Étape 2 Affectez l'interface à un groupe de ponts :

bridge-group *number*

Exemple :

```
ciscoasa(config-if)# bridge-group 1
```

Le *nombre* est un entier compris entre 1 et 250 et doit correspondre au numéro d'interface BVI. Vous pouvez attribuer jusqu'à 64 interfaces à un groupe de ponts. Vous ne pouvez pas attribuer la même interface à plusieurs groupes de ponts.

Étape 3 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif inside1
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 4 Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Le paramètre *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Sujets connexes

Configurer , la et le TCP MSS, à la page 809

Configurer une interface de gestion pour le mode transparent

En mode de pare-feu transparent, toutes les interfaces doivent appartenir à un groupe de ponts. La seule exception est l'interface de gestion (l'interface physique, une sous-interface (si prise en charge pour votre modèle) ou une interface EtherChannel composée d'interfaces de gestion (si vous avez plusieurs interfaces de gestion)) que vous pouvez configurer en tant qu'interface de gestion distincte; pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA. Vous ne pouvez pas utiliser d'autres types d'interfaces comme interfaces de gestion. Vous pouvez configurer une interface de gestion en mode unique ou par contexte. Pour obtenir plus de renseignements, consultez Interface de gestion pour le mode transparent, à la page 673.

L'interface de gestion traite uniquement le trafic entrant et sortant et ne peut pas transmettre de trafic de transit.

Avant de commencer

- N'attribuez pas cette interface à un groupe de ponts; un groupe de ponts non configurable (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.
- Pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA.
- En mode de contexte multiple, vous ne pouvez partager aucune interface, y compris l'interface de gestion, entre les contextes. Vous devez vous connecter à une interface de données.
- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez la commande **changeto context** *name*.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface {{**port-channel** *number* | **management** *slot*/*port* | *mgmt-type_interface_id* }[**.** *subinterface*] | *mapped_name*}

Exemple :

```
ciscoasa(config)# interface management 0/0.1
```

L'argument **port-channel** *number* est l'ID de l'interface EtherChannel, tel que **port-channel 1**. L'interface EtherChannel ne doit avoir que des interfaces membres de gestion.

En mode de contexte multiple, saisissez le *mapped_name* s'il a été attribué à l'aide de la commande **allocate-interface**.

Pour le Châssis Firepower 4100/9300 , spécifiez l'ID d'interface pour l'interface de type de gestion (individuelle ou EtherChannel) que vous avez attribuée au périphérique logique ASA.

Étape 2 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif management
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 3 Définissez l'adresse IP à l'aide de l'une des méthodes suivantes.

- Définissez l'adresse IP manuellement :

  Pour une utilisation avec le basculement, vous devez définir manuellement l'adresse IP et l'adresse en veille; le protocole DHCP n'est pas pris en charge.

  Les arguments *ip_address* et *mask* définissent l'adresse IP de l'interface et le filtre d'adresse locale.

  L'argument *ip_address* en veille est utilisé pour le basculement.

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

- Obtenez une adresse IP à partir d'un serveur DHCP :

  ip address dhcp [**setroute**]

  Exemple :

```
ciscoasa(config-if)# ip address dhcp
```

Le mot clé **setroute** permet à l'ASA d'utiliser la route par défaut fournie par le serveur DHCP.

Saisissez à nouveau cette commande pour réinitialiser le bail locatif DHCP et demander un nouveau bail locatif.

Si vous n'activez pas l'interface à l'aide de la commande no shutdown avant de saisir la commande **ip address dhcp**, certaines demandes DHCP pourraient ne pas être envoyées.

Étape 4 Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 100
```

Le paramètre *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Configuration de l'adressage IPv6

Cette section décrit comment configurer l'adressage IPv6.

À propos d'IPv6

Cette section comprend des informations sur IPv6.

Adresse IPv6

Vous pouvez configurer deux types d'adresses de monodiffusion pour IPv6 :

- Adresse globale (global) : l'adresse globale est une adresse publique que vous pouvez utiliser sur le réseau public. Pour un groupe de ponts, cette adresse doit être configurée pour les BVI, et non par interface membre. Vous pouvez également configurer une adresse IPv6 globale pour l'interface de gestion en mode transparent.
- Adresse locale du lien (link-local) : l'adresse locale du lien est une adresse privée que vous ne pouvez utiliser que sur le réseau directement connecté. Les routeurs ne transfèrent pas les paquets en utilisant des adresses locales du lien; ils sont uniquement destinés à la communication sur un segment de réseau physique donné. Ils peuvent être utilisés pour la configuration des adresses ou pour les fonctions de découverte du voisin telles que la résolution d'adresses. Dans un groupe de ponts, seules les interfaces membres ont des adresses de lien locales; les BVI n'ont pas d'adresse locale de lien.

Au minimum, vous devez configurer une adresse locale de lien pour que IPv6 fonctionne. Si vous configurez une adresse globale, une adresse locale de lien est automatiquement configurée sur l'interface, vous n'avez donc pas besoin de configurer spécifiquement une adresse locale de lien. Pour les interfaces membres des groupes de ponts, lorsque vous configurez l'adresse globale sur les BVI, ASA génère automatiquement des adresses link-local pour les interfaces membres. Si vous ne configurez pas d'adresse globale, vous devez configurer l'adresse locale de lien. La configuration peut s'effectuer automatiquement ou manuellement.

Remarque Si vous souhaitez configurer uniquement les adresses link-local, consultez la commande **ipv6 Enable** (pour la configuration automatique) ou **ipv6 address link-local** (pour la configuration manuelle) dans la référence de commandes.

ID d'interface EUI-64 modifiées

RFC 3513 : IPv6 (Internet Protocol Version 6) exige que la partie identifiant d'interface de toutes les adresses IPv6 de monodiffusion, à l'exception de celles qui commencent par la valeur binaire 000, ait une longueur de 64 bits et soit bâtie au format EUI-64 modifié. L'ASA peut appliquer cette exigence pour les hôtes associés au lien local.

Lorsque cette fonctionnalité est activée sur une interface, les adresses source des paquets IPv6 reçus sur cette interface sont comparées aux adresses MAC sources pour s'assurer que les identifiants d'interface utilisent le format EUI-64 modifié. Si les paquets IPv6 n'utilisent pas le format EUI-64 modifié comme identifiant d'interface, les paquets sont abandonnés et le message de journal système suivant est généré :

```
325003: EUI-64 source address check failed.
```

La vérification du format de l'adresse n'est effectuée que lors de la création d'un flux. Les paquets d'un flux existant ne sont pas vérifiés. De plus, la vérification de l'adresse ne peut être effectuée que pour les hôtes du lien local.

Configurer le client de délégation de préfixe IPv6

Le ASA peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que le ASA peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes.

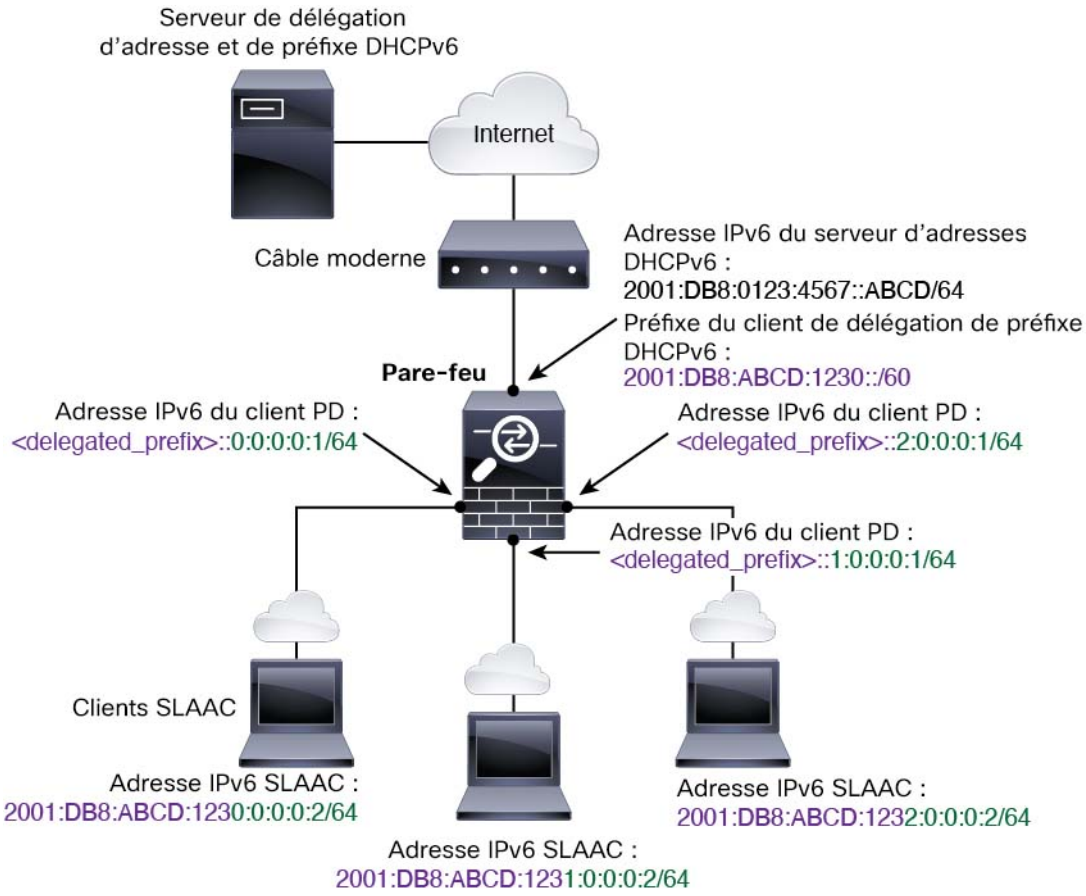
À propos de la délégation de préfixe IPv6

Le ASA peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que le ASA peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes. Les hôtes connectés aux interfaces internes peuvent ensuite utiliser la configuration automatique sans état (SLAAC) pour obtenir des adresses IPv6 globales. Notez que les interfaces ASA internes n'agissent pas à leur tour comme des serveurs de délégation de préfixe; Le ASA ne peut fournir des adresses IP globales qu'aux clients SLAAC. Par exemple, si un routeur est connecté à l'ASA, il peut agir en tant que client SLAAC pour obtenir son adresse IP. Mais si vous souhaitez utiliser un sous-réseau du préfixe délégué pour les réseaux derrière le routeur, vous devez configurer manuellement ces adresses sur les interfaces internes du routeur.

L'ASA comprend un serveur DHCPv6 léger, de sorte que l'ASA peut fournir des informations telles que le serveur DNS et le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que ASA a reçu à l'aide de la délégation de préfixe.

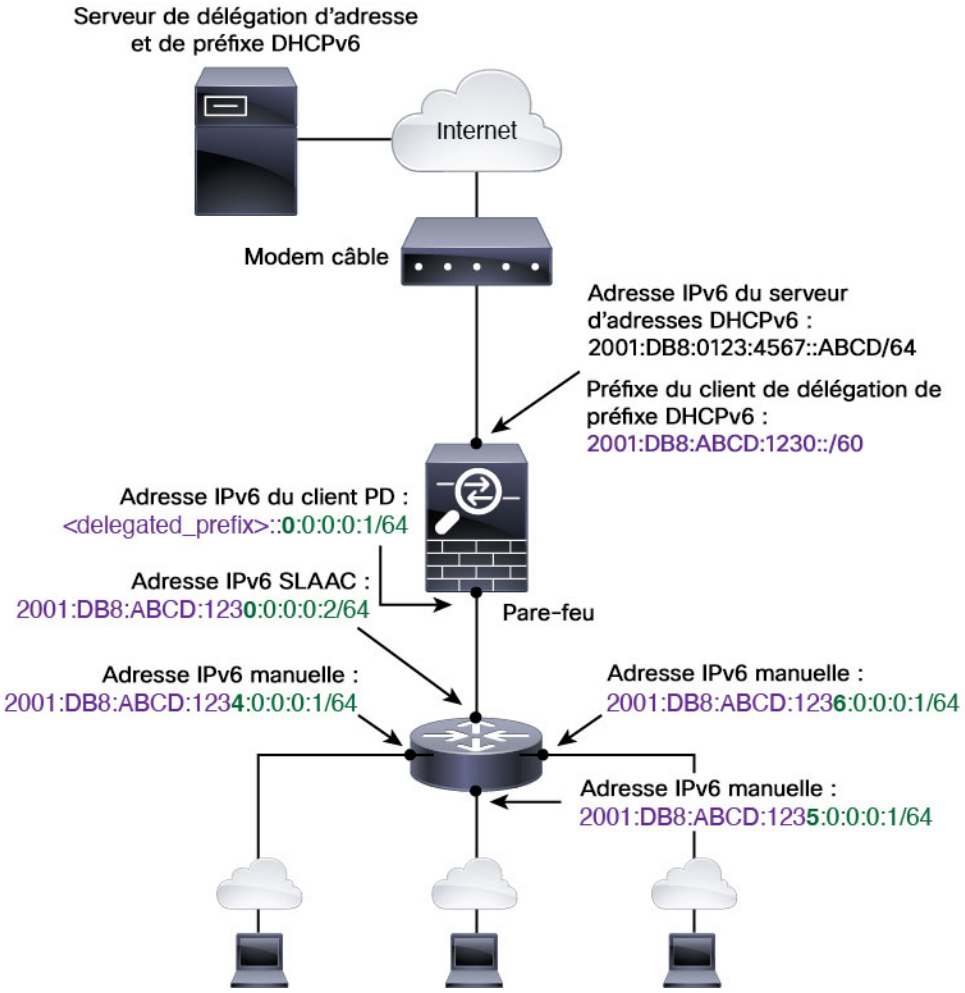
Exemple de délégation de préfixe IPv6 /de sous-réseau 64

L'exemple suivant montre que ASA reçoit une adresse IP sur l'interface externe en utilisant l'adresse DHCPv6. Il obtient également un préfixe délégué à l'aide du client de délégation de préfixe DHCPv6. Le ASA subdivise le préfixe délégué en réseaux /64 et attribue des adresses IPv6 globales à ses interfaces internes de manière dynamique en utilisant le préfixe délégué plus un sous-réseau configuré manuellement (::0, ::1 ou ::2) et une adresse IPv6 (0:0:0:1) par interface. Les clients SLAAC connectés à ces interfaces internes obtiennent des adresses IPv6 sur chaque sous-réseau /64.



Exemple de délégation de préfixe IPv6 /de sous-réseau 62

L'exemple suivant montre la sous-réseaux ASA du préfixe en 4 sous-réseaux /62 : 2001:DB8:ABCD:123**0**:/62, 2001:DB8:ABCD:123**4**:/62, 2001:DB8:ABCD:123**8**::/62 et 2001:DB8:ABCD:123 **C**::/62. ASA utilise l'un des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1230::/62 pour son réseau interne (::0). Vous pouvez ensuite utiliser manuellement des sous-réseaux /62 supplémentaires pour les routeurs en aval. Le routeur illustré utilise 3 des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1234::/62 pour ses interfaces internes (::4,::5 et::6). Dans ce cas, les interfaces de routeur internes ne peuvent pas obtenir dynamiquement le préfixe délégué. Vous devez donc afficher le préfixe délégué sur ASA, puis utiliser ce préfixe pour la configuration de votre routeur. Habituellement, les fournisseurs de services Internet délèguent le même préfixe à un client donné à l'expiration du bail, mais si ASA reçoit un nouveau préfixe, vous devrez modifier la configuration du routeur pour utiliser le nouveau préfixe. L'identifiant unique (DUID) de DHCP est persistant pendant les redémarrages.



Activer le client de délégation de préfixe IPv6

Activez le client de délégation de préfixe DHCPv6 sur une ou plusieurs interfaces. L'ASA obtient un ou plusieurs préfixes IPv6 qu'elle peut subdiviser en sous-réseaux et attribuer à des réseaux internes. En règle générale, l'interface sur laquelle vous activez la délégation de préfixe client obtient son adresse IP à l'aide de l'adresse client DHCPv6; Seules les autres interfaces ASA utilisent des adresses dérivées du préfixe délégué.

Avant de commencer

- Cette fonction n'est prise en charge qu'en mode pare-feu routé.
- Cette fonctionnalité n'est pas prise en charge en mode contexte multiple.
- Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe.
- Vous ne pouvez pas configurer cette fonction sur une interface de gestion uniquement.
- Lorsque vous utilisez la délégation de préfixe, vous devez définir l'intervalle d'annonce du routeur de découverte des voisins IPv6 de l'ASA de manière à ce qu'il soit bien inférieur à la durée de vie souhaitée du préfixe attribué par le serveur DHCPv6, afin d'éviter toute interruption du trafic IPv6. Par exemple, si le serveur DHCPv6 définit la durée de vie préférée de délégation de préfixe à 300 secondes, vous devez

définir l'intervalle d'annonce de routeur de l'ASA à 150 secondes. Pour définir la durée de vie préférée, utilisez la commande **show ipv6 general-prefix**. Pour définir l'intervalle d'annonce de routeur de l'ASA, consultez Configurer la découverte des voisins IPv6, à la page 786; la valeur par défaut est de 200 secondes.

Procédure

Étape 1 Passez en mode de configuration d'interface pour l'interface connectée au réseau du serveur DHCPv6 :

interface *ID*

Exemple :

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

Étape 2 Activez le client DHCPv6 Prefix Delegation et nommez le(s) préfixe(s) obtenu(s) sur cette interface :

ipv6 dhcp client pd *name*

Exemple :

```
ciscoasa(config-if)# ipv6 dhcp client pd Outside-Prefix
```

Le *nom* peut comporter jusqu'à 200 caractères.

Étape 3 Fournissez un ou plusieurs conseils sur le préfixe délégué que vous souhaitez recevoir :

ipv6 dhcp client pd hint *ipv6_prefix/prefix_length*

Exemple :

```
ciscoasa(config-if)# ipv6 dhcp client pd hint 2001:DB8:ABCD:1230::/60
```

En règle générale, vous souhaitez demander une longueur de préfixe particulière, telle que ::/60, ou si vous avez déjà reçu un préfixe particulier et que vous souhaitez vous assurer de le recevoir à nouveau à l'expiration du bail, vous pouvez saisir le préfixe complet comme conseil. Si vous saisissez plusieurs conseils (préfixes ou longueurs différents), il appartient au serveur DHCP de choisir de respecter le conseil ou non.

Étape 4 Consultez Configuration d'une adresse globale IPv6, à la page 783 pour affecter un sous-réseau du préfixe comme adresse IP globale pour une interface ASA.

Étape 5 (Facultatif) Consultez Configurer le serveur sans état DHCPv6, à la page 865 pour fournir le nom de domaine et les paramètres de serveur aux clients SLAAC.

Étape 6 (Facultatif) Consultez Configurer les paramètres réseau IPv6, à la page 1031 pour annoncer le ou les préfixes avec BGP.

Exemple

Dans l'exemple suivant, le client d'adresse DHCPv6 et le client de délégation de préfixe sont configurés sur GigabitEthernet 0/0, puis attribuent les adresses avec le préfixe sur les GigabitEthernet 0/1 et 0/2 :

```
interface gigabitethernet 0/0
  ipv6 address dhcp default
  ipv6 dhcp client pd Outside-Prefix
  ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Configuration d'une adresse globale IPv6

Pour configurer une adresse IPv6 globale pour une interface en mode routé et pour le BVI en mode transparent ou routé, procédez comme suit.

Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode de contexte multiple.

Remarque La configuration de l'adresse globale configure automatiquement l'adresse de lien local, de sorte que vous n'avez pas besoin de la configurer séparément. Pour les groupes de ponts, la configuration de l'adresse globale sur les BVI configure automatiquement les adresses de lien locales sur toutes les interfaces membres.

Pour les sous-interfaces, nous vous recommandons de définir également l'adresse MAC manuellement, car elles utilisent la même adresse MAC gravée de l'interface parente. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur l'ASA. Consultez Configurer manuellement l'adresse MAC, à la page 807.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *ID*

Exemple :

```
ciscoasa(config)# interface gigabithethernet 0/0
```

En mode transparent ou pour un groupe de ponts en mode routé, spécifiez le BVI :

Exemple :

```
ciscoasa(config)# interface bvi 1
```

En mode transparent, en plus des BVI, vous pouvez également spécifier une interface de gestion :

Exemple :

```
ciscoasa(config)# interface management 1/1
```

Étape 2 (interface routée) Définissez l'adresse IP à l'aide de l'une des méthodes suivantes.

Pour le basculement et la mise en grappe, ainsi que pour les interfaces de boucle avec retour, vous devez définir l'adresse IP manuellement. Pour la mise en grappe, la configuration manuelle de l'adresse Link-Local n'est pas prise en charge.

- Activez l'autoconfiguration d'adresse sans état (SLAAC) sur l'interface :

  ipv6 address autoconfig [**default trust** {**dhcp** | **ignore**}]

  L'activation de la SLAAC sur l'interface configure les adresses IPv6 en fonction des préfixes reçus dans les messages d'annonce de routeur. Une adresse Link-Local, basée sur l'ID d'interface EUI-64 modifiée, est automatiquement générée pour l'interface lorsque la SLAAC est activée.

  Remarque
  Bien que la RFC 4862 spécifie que les hôtes configurés pour une SLAAC n'envoient pas de messages d'annonce de routeur, l'ASA envoie ces messages dans ce cas. Consultez la commande **ipv6 nd suppress-ra** pour supprimer les messages.

  Si vous souhaitez installer une voie de routage par défaut, spécifiez **default trust dhcp** ou **ignore**. **dhcp** précise que l'ASA utilise uniquement une voie de routage par défaut des annonces de routeur qui proviennent d'une source de confiance (c'est-à-dire du même serveur qui a fourni l'adresse IPv6). **ignore** spécifie que les annonces de routeur peuvent provenir d'un autre réseau, ce qui peut être une méthode plus risquée.

- Obtenez une adresse à l'aide de DHCPv6 :

  ipv6 address dhcp [**default**]

  Exemple :

  ```
  ciscoasa(config-if)# ipv6 address dhcp default
  ```

  Le mot clé **default** obtient une voie de routage par défaut à partir des publicités de routeur.

- Attribuez manuellement une adresse globale à l'interface :

  ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

  Exemple :

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
  ```

Lorsque vous attribuez une adresse globale, l'adresse locale du lien est automatiquement créée pour l'interface.

standby (veille/secours) spécifie l'adresse d'interface utilisée par l'unité secondaire ou le groupe de basculement dans une paire de basculement.

- Attribuez une adresse globale à l'interface en combinant le préfixe spécifié avec un ID d'interface généré à partir de l'adresse MAC d'interface au moyen du format EUI-64 modifié :

  ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

  Exemple :

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
  ```

  Lorsque vous attribuez une adresse globale, l'adresse locale du lien est automatiquement créée pour l'interface.

  Vous n'avez pas besoin de préciser l'adresse de secours; l'ID d'interface sera généré automatiquement.

- Utilisez un préfixe délégué :

  ipv6 address *prefix_name ipv6_address*/*prefix_length*

  Exemple :

  ```
  ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ```

  Cette fonctionnalité exige que l'ASA ait activé la délégation de préfixe DHCPv6 *sur une interface différente*. Consultez Activer le client de délégation de préfixe IPv6, à la page 781. En règle générale, le préfixe délégué est /60 ou moins, de sorte que vous pouvez créer un sous-réseau à plusieurs réseaux /64. /64 est la longueur de sous-réseau prise en charge si vous souhaitez prendre en charge SLAAC pour les clients connectés. Vous devez spécifier une adresse qui complète le sous-réseau /60, par exemple ::1:0:0:0:1. Saisissez : avant l'adresse si le préfixe est inférieur à 60. Par exemple, si le préfixe délégué est 2001:DB8:1234:5670::60, l'adresse IP globale attribuée à cette interface est 2001:DB8:1234:5671::1/64. Le préfixe annoncé dans les annonces des routeurs est 2001:DB8:1234:5671::/64. Dans cet exemple, si le préfixe est inférieur à 60, les bits restants du préfixe seront des 0, comme l'indique le préfixe::. Par exemple, si le préfixe est 2001:DB8:1234::/48, l'adresse IPv6 sera 2001:DB8:1234::1:0:0:0:1/64.

Étape 3 (interface BVI) Attribuez manuellement une adresse globale aux BVI. Pour une interface de gestion en mode transparent, utilisez également cette méthode.

ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

Exemple :

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

Lorsque vous attribuez une adresse globale, l'adresse locale du lien est automatiquement créée pour l'interface.

standby (veille/secours) spécifie l'adresse d'interface utilisée par l'unité secondaire ou le groupe de basculement dans une paire de basculement.

Étape 4 (Facultatif) Appliquer l'utilisation d'identifiants d'interface au format EUI-64 modifié dans les adresses IPv6 sur un lien local :

ipv6 enforce-eui64 *if_name*

Exemple :

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

L'argument *if_name* est le nom de l'interface, comme spécifié par la commande **nameif**, sur laquelle vous activez l'application du format d'adresse.

Configurer la découverte des voisins IPv6

Le processus de découverte des voisins IPv6 utilise des messages ICMPv6 et des adresses de multidiffusion de nœud sollicité pour déterminer l'adresse de couche de liaison d'un voisin sur le même réseau (lien local), vérifier la lisibilité d'un voisin et suivre les routeurs voisins.

Les nœuds (hôtes) utilisent la découverte des voisins pour déterminer les adresses de couche de liaison des voisins connus pour résider sur les liens attachés et pour purger rapidement les valeurs en cache qui deviennent non valides. Les hôtes ont également recours à la découverte des voisins pour trouver les routeurs voisins qui sont prêts à transférer des paquets en leur nom. En outre, les nœuds utilisent le protocole pour garder activement une trace des voisins accessibles et de ceux qui ne le sont pas, et pour détecter les adresses de couche de liaison modifiées. Lorsqu'un routeur ou le chemin d'accès à un routeur tombe en panne, un hôte recherche activement des solutions de remplacement qui fonctionnent.

Procédure

Étape 1 Précisez l'interface IPv6 que vous souhaitez configurer.

interface *name* (Nom d'interface)

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)#
```

Étape 2 Précisez le nombre de tentatives de détection d'adresses en double (DAD).

ipv6 nd dad attempts *value*

Les valeurs valides pour l'argument *value* sont comprises entre 0 et 600. La valeur 0 désactive le traitement de la DAD sur l'interface spécifiée. La valeur par défaut est de 1 message par seconde.

DAD garantit l'unicité des nouvelles adresses IPv6 de monodiffusion avant qu'elles ne soient attribuées et veille à ce que les adresses IPv6 en double soient détectées dans le réseau selon les liaisons. Le ASA utilise les messages de sollicitation des voisins pour effectuer le DAD.

Lorsqu'une adresse en double est identifiée, l'état de l'adresse est défini à DUPLICATE, l'adresse n'est pas utilisée et le message d'erreur suivant est généré :

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

Si l'adresse en double est l'adresse link-local de l'interface, le traitement des paquets IPv6 est désactivé sur l'interface. Si l'adresse en double est une adresse globale, l'adresse n'est pas utilisée.

Exemple :

```
ciscoasa(config-if)# ipv6 nd dad attempts 20
```

Étape 3 Définissez l'intervalle entre les retransmissions de sollicitation d'un voisin IPv6.

ipv6 nd ns-interval *value*

Les valeurs de l'argument *value* sont comprises entre 1000 et 3600000 millisecondes.

Les messages de sollicitation des voisins (ICMPv6 de type 135) sont envoyés sur la liaison locale par les nœuds qui tentent de découvrir les adresses de couche de liaison d'autres nœuds sur la liaison locale. Après avoir reçu un message de sollicitation de voisin, le nœud de destination répond en envoyant un message d'annonce de voisin (ICPMv6 type 136) sur la liaison locale.

Une fois que le nœud source a reçu l'annonce de voisin, le nœud source et le nœud de destination peuvent communiquer. Les messages de sollicitation de voisin sont également utilisés pour vérifier l'accessibilité d'un voisin après avoir identifié l'adresse de couche de liaison d'un voisin. Lorsqu'un nœud souhaite vérifier l'accessibilité d'un voisin, l'adresse de destination dans un message de sollicitation de voisin est l'adresse de monodiffusion du voisin.

Des messages d'annonce de voisin sont également envoyés en cas de changement dans l'adresse de couche de liaison d'un nœud sur une liaison locale.

Exemple :

```
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

Étape 4 Définissez la durée pendant laquelle un nœud IPv6 distant est accessible.

ipv6 nd reachable-time *value*

Les valeurs de l'argument *value* sont comprises entre 0 et 3600000 millisecondes. Lorsque 0 est utilisé pour la valeur, la durée accessible est envoyée comme indéterminée. Il appartient aux périphériques de réception de définir et de suivre la durée accessible.

La durée d'accessibilité du voisin permet de détecter les voisins non disponibles. Des durées configurées plus courtes permettent de détecter plus rapidement les voisins non disponibles, mais des durées plus courtes consomment plus de bande passante réseau IPv6 et de ressources de traitement dans tous les périphériques réseau IPv6. Des durées configurées très courtes ne sont pas recommandées pour le fonctionnement normal d'un IPv6.

Exemple :

```
ciscoasa config-if)# ipv6 nd reachable-time 1700000
```

Étape 5 Définissez l'intervalle entre les transmissions des annonces du routeur IPv6.

ipv6 nd ra-interval [**msec**] *value*

Le mot clé **msec** indique que la valeur fournie est en millisecondes. Si ce mot clé n'est pas présent, la valeur fournie est en secondes. Les valeurs valides pour l'argument *value* sont comprises entre 3 et 1 800 secondes ou entre 500 et 1 800 000 millisecondes si le mot clé **msec** est fourni. La valeur par défaut est de 200 secondes.

La valeur d'intervalle est incluse dans toutes les annonces de routeur IPv6 qui sont envoyées à partir de cette interface.

L'intervalle entre les transmissions doit être inférieur ou égal à la durée de vie des annonces du routeur IPv6 si l'ASA est configuré comme routeur par défaut.

Pour empêcher la synchronisation avec d'autres nœuds IPv6, l'ASA ajuste de manière aléatoire la valeur que vous avez définie (gigue).

Exemple :

```
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

Étape 6 Spécifiez la durée pendant laquelle les nœuds de la liaison locale doivent considérer l'ASA comme routeur par défaut sur la liaison.

ipv6 nd ra-lifetime [**msec**] *value*

Le mot clé facultatif **msec** indique que la valeur fournie est en millisecondes. Sinon, la valeur est en secondes. Les valeurs de l'argument *value* sont comprises entre 0 et 9 000 secondes. Si la valeur 0 est saisie, l'ASA ne doit pas être considéré comme un routeur par défaut sur l'interface sélectionnée.

La valeur de vie du routeur est incluse dans toutes les annonces de routeur IPv6 envoyées hors de l'interface. La valeur indique l'utilité de l'ASA en tant que routeur par défaut sur cette interface.

Exemple :

```
ciscoasa(config-if)# ipv6 nd ra-lifetime 2000
```

Étape 7 Supprimer les annonces du routeur.

ipv6 nd suppress-ra

Les messages d'annonce de routeur (ICMPv6 Type 134) sont automatiquement envoyés en réponse aux messages de sollicitation de routeur (ICMPv6 Type 133). Les messages de sollicitation de routeur sont envoyés par les hôtes au démarrage du système, ce qui permet à l'hôte de se configurer automatiquement sans avoir à attendre le prochain message de publicité de routeur planifié.

Vous pouvez souhaiter désactiver ces messages sur toute interface pour laquelle vous ne souhaitez pas que l'ASA fournisse le préfixe IPv6 (par exemple, l'interface extérieure).

Cette commande fait que l'ASA s'affiche comme un voisin IPv6 standard sur la liaison et non comme un routeur IPv6.

Étape 8 Ajoutez un indicateur aux annonces de routeur IPv6 pour informer les clients d'autoconfiguration d'adresse sans état (SLAAC) IPv6 d'utiliser DHCPv6 pour obtenir une adresse IPv6, en plus de l'adresse SLAAC dérivée.

ipv6 nd managed-config-flag

Cette option définit l'indicateur de configuration d'adresse gérée dans le paquet d'annonce du routeur IPv6.

Étape 9 Ajoutez un indicateur aux annonces de routeur IPv6 pour informer les clients SLAAC IPv6 d'utiliser DHCPv6 pour obtenir l'adresse du serveur DNS ou d'autres renseignements.

ipv6 nd other-config-flag

Cette option définit l'indicateur Another Address Config (Configuration d'une autre adresse) dans le paquet d'annonce du routeur IPv6.

Étape 10 Configurez quels préfixes IPv6 sont inclus dans les annonces de routeur IPv6 :

ipv6 nd prefix {*ipv6_prefix*/*prefix_length* | **default**} [*valid_lifetime preferred_lifetime* | **at** *valid_date preferred_date*] [**no-advertise**] [**no-autoconfig**] [ ] [**off-link**]

L'annonce de préfixe peut être utilisée par les périphériques voisins pour configurer automatiquement leurs adresses d'interface. SLAAC utilise les préfixes IPv6 fournis dans les messages d'annonce des routeurs pour créer l'adresse de monodiffusion globale à partir de l'adresse Link-Local.

Par défaut, les préfixes configurés comme adresses sur une interface à l'aide de la commande **d'adresse ipv6** sont annoncés dans les annonces de routeur. Si vous configurez des préfixes pour publication à l'aide de la commande **ipv6 nd prefix**, seuls ces préfixes sont annoncés.

Pour que SLAAC fonctionne correctement, la longueur du préfixe annoncée dans les messages d'annonce du routeur doit toujours être de 64 bits.

- **default** : pour indiquer que le préfixe par défaut est utilisé.
- *valid_lifetime preferred_lifetime* : spécifie la durée pendant laquelle le préfixe IPv6 spécifié est annoncé comme valide et préféré. Une adresse n'a aucune restriction pendant sa durée de vie préférée. À l'expiration de la durée de vie préférée, l'adresse passe à l'état obsolète. Lorsqu'une adresse est dans un état obsolète, son utilisation est déconseillée, mais pas formellement interdite. Après l'expiration de la durée de vie valide, l'adresse devient non valide et ne peut pas être utilisée. La durée de vie valide doit être supérieure ou égale à la durée de vie préférée. Les valeurs sont comprises entre 0 et 4294967295 secondes. La valeur maximale représente l'éternité, et peut également être spécifiée à l'aide du mot clé **infinite**. La valeur par défaut de la durée de vie valide est de 2 592 000 (30 jours). La durée de vie par défaut préférée est 604 800 (7 jours).
- **at** *valid_date preferred_date* : indique une date et une heure spécifiques à laquelle le préfixe expire. Spécifiez la date au format *mois_jour hh*:*mm*. Par exemple, saisissez **déc 1 13:00**.
- **no-advertise** : pour désactiver l'annonce du préfixe. Pour le préfixe **default**, ce paramètre s'applique uniquement aux préfixes sur la liaison. Les préfixes hors liaison seront toujours annoncés, sauf si vous spécifiez **no-advertise** pour un préfixe hors liaison précis.
- **no-autoconfig** : spécifie que le préfixe ne peut pas être utilisé pour SLAAC IPv6.
- **off-link** : pour configurer le préfixe spécifié comme hors liaison. Le préfixe sera annoncé avec le bit L en effacement. Le préfixe ne sera pas inséré dans la table de routage en tant que préfixe connecté.

  Lorsque onlink est activé (par défaut), le préfixe spécifié est affecté au lien. Les nœuds envoyant du trafic vers de telles adresses qui contiennent le préfixe spécifié considèrent la destination comme accessible localement sur le lien.

Exemple :

```
ciscoasa(config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

Étape 11 Configurez une entrée statique dans le cache de découverte des voisins IPv6.

ipv6 neighbor *ipv6_address if_name mac_address*

Les directives et limites suivantes s'appliquent à la configuration d'un voisin IPv6 statique :

- La commande **ipv6 neighbor** est similaire à la commande **arp**. Si une entrée pour l'adresse IPv6 précisée existe déjà dans le cache de découverte des voisins (apprise par le processus de découverte des voisins IPv6), elle est automatiquement convertie en entrée statique. Ces entrées sont stockées dans la configuration lorsque la commande copy est utilisée pour stocker la configuration.
- Utilisez la commande **show ipv6 neighbor** pour afficher les entrées statiques dans le cache de découverte IPv6 neighbor.
- La commande **clear ipv6 neighbor** supprime toutes les entrées du cache de découverte IPv6 neighbor, à l'exception des entrées statiques. La commande **no ipv6 neighbor** supprime une entrée statique spécifiée de la mémoire cache de découverte du voisin; la commande ne supprime pas les entrées dynamiques (les entrées apprises du processus de découverte des voisins IPv6) du cache. La désactivation d'IPv6 sur une interface à l'aide de la commande **no ipv6 enable** supprime toutes les entrées du cache de découverte des voisins IPv6 configurées pour cette interface, à l'exception des entrées statiques (l'état de l'entrée passe à INCMP [Incomplete]).
- Les entrées statiques de la mémoire cache de découverte du voisin IPv6 ne sont pas modifiées par le processus de découverte du voisin.
- La commande **clear ipv6 neighbor** ne supprime pas les entrées statiques de la mémoire cache de découverte IPv6 neighbor; il efface uniquement les entrées dynamiques.
- Les journaux système ICMP générés sont provoqués par une actualisation régulière des entrées IPv6 neighbor. La minuterie par défaut de l'ASA pour l'entrée du voisin IPv6 est de 30 secondes, donc l'ASA génère des paquets de découverte et de réponse des voisins ICMPv6 toutes les 30 secondes. Si l'ASA est dotée d'interfaces LAN et d'état de basculement configurées avec des adresses IPv6, toutes les 30 secondes, des paquets de réponse et de découverte de voisin ICMPv6 seront générés par les deux ASA pour les adresses IPv6 configurées et celles liées au lien local. En outre, chaque paquet génère plusieurs syslogs (connexion ICMP et création ou démontage de l'hôte local), de sorte qu'il peut sembler que des syslogs ICMP sont générés en permanence. L'heure d'actualisation de l'entrée du voisin IPV6 peut être configurée sur l'interface de données normale, mais pas sur l'interface de basculement. Cependant, l'impact sur le CPU pour ce trafic de découverte de voisin ICMP est minime.

Exemple :

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

Supervision des interfaces en mode routé et en mode transparent

Vous pouvez superviser les statistiques d'interface, l'état, PPPoE

Remarque Pour les modèles Firepower et Secure Firewall, certaines statistiques ne sont pas affichées à l'aide des commandes ASA. Vous devez consulter des statistiques d'interface plus détaillées à l'aide des commandes FXOS.

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

Pour Firepower 2100 en mode plateforme, consultez aussi les commandes FXOS connect local-mgmt suivantes :

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

Consultez le guide de dépannage FXOS pour plus d'informations.

Statistiques et informations sur l'interface

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

- **show bridge-group**

  Affiche les renseignements sur le groupe de ponts, comme les interfaces attribuées, les adresses MAC et les adresses IP.

Renseignements sur DHCP

- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  La commande **show ipv6 dhcp interface** affiche les renseignements DHCPv6 pour toutes les interfaces. Si l'interface est configurée pour la configuration du serveur sans état DHCPv6 (voir Configurer le serveur sans état DHCPv6, à la page 865), cette commande répertorie l'ensemble DHCPv6 utilisé par le serveur. Si l'interface a une configuration de client d'adresse DHCPv6 ou de client de délégation de préfixe, cette commande affiche l'état de chaque client et les valeurs reçues du serveur. Pour une interface en particulier, vous pouvez afficher les statistiques des messages pour le serveur ou le client DHCP. Les exemples suivants montrent les renseignements fournis par cette commande :

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
```

```
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:
```

```
 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp client** [**pd**] **statistics**

  La commande **show ipv6 dhcp client statistics** affiche les statistiques du client DHCPv6 et indique le résultat du nombre de messages envoyés et reçus. La commande **show ipv6 dhcp client pd statistics** affiche les statistiques du client de délégation de préfixes. Les exemples suivants montrent les renseignements fournis par cette commande :

```
ciscoasa(config)# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                   8
  Total number of Message Validation errors in received messages: 0


ciscoasa(config)# show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:
```

```
 Total number of Re-transmission messages sent:                 1
 Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  La commande **show ipv6 dhcp ha statistics** affiche les statistiques de transaction entre les unités de basculement, y compris le nombre de fois où les renseignements DUID ont été synchronisés entre les unités. Les exemples suivants montrent les renseignements fournis par cette commande.

  Sur une unité active :

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:             1
  DUID sync messages received:         0

DHCPv6 HA error statistics:
  Send errors:                         0
```

  Sur une unité de secours :

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:             0
  DUID sync messages received:         1

DHCPv6 HA error statistics:
  Send errors:                         0
```

- **show ipv6 general-prefix**

  La commande **show ipv6 general-prefix** affiche tous les préfixes acquis par les clients de délégation de préfixe DHCPv6 et la distribution ASA de ce préfixe à d'autres processus (« Liste des consommateurs »). L'exemple suivant montre les renseignements fournis par cette commande :

```
ciscoasa(config)# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List               Usage count
    BGP network command        1
    inside (Address command)   1
```

PPPoE

- **show ip address** *interface_name* **pppoe**

  Affiche les renseignements de configuration actuels du client PPPoE.

- **debug pppoe** {**event** | **error** | **packet**}

  Active le débogage pour le client PPPoE.

- **show vpdn session** [**l2tp** | **pppoe**] [**id** *sess_id* | **packets** | **state** | **window**]

Affiche l'état des sessions PPPoE.

Les exemples suivants montrent les renseignements fournis par cette commande :

```
ciscoasa# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
```

Découverte de voisin IPv6

Pour superviser les paramètres de découverte de voisin IPv6, saisissez les commandes suivantes.

- **show ipv6 interface**

  Cette commande affiche l'état de convivialité des interfaces configurées pour IPv6, y compris le nom de l'interface, tel que « externe », et affiche les paramètres de l'interface spécifiée. Cependant, elle exclut le nom de la commande et affiche les paramètres de toutes les interfaces sur lesquelles IPv6 est activé. La sortie de la commande affiche les éléments suivants :

  - Le nom et l'état de l'interface.
  - Les adresses de monodiffusion Link-Local et globale.
  - Les groupes de multidiffusion auxquels appartient l'interface.
  - Les paramètres de redirection ICMP et de message d'erreur.
  - Les paramètres du protocole ndp (Neighbor Discovery Protocol)
  - L'heure réelle à laquelle la commande est définie sur 0.
  - L'heure d'accessibilité utilisée pour la découverte du voisin.

Exemples d'interfaces en mode routé et en mode transparent

Exemple de mode transparent avec 2 groupes de ponts

L'exemple suivant de mode transparent comprend deux groupes de ponts de trois interfaces chacun, plus une interface de gestion uniquement :

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

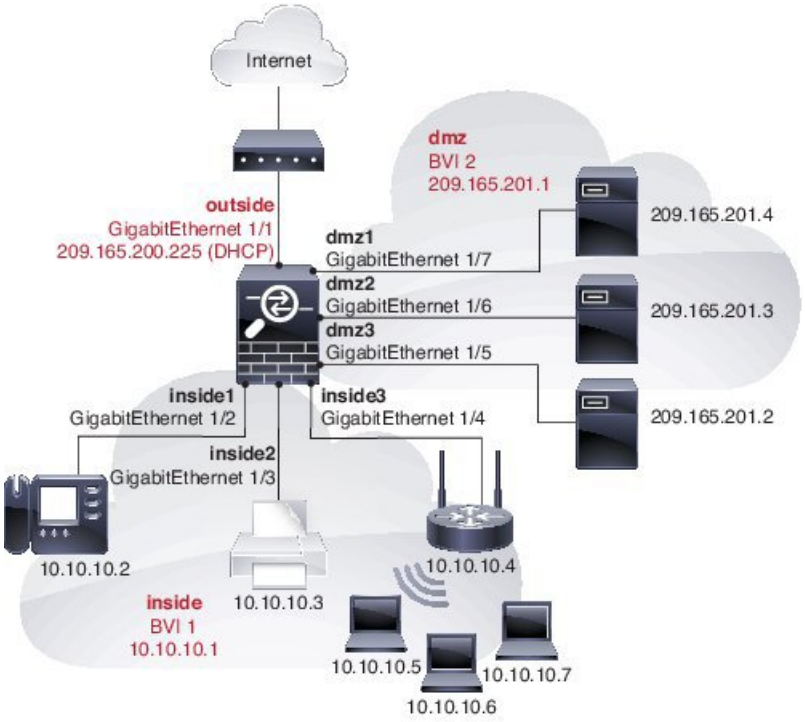
interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

Exemple de segment LAN commuté avec 2 groupes de ponts

Dans l'exemple suivant, deux groupes de ponts de 3 interfaces et une interface routée standard pour l'extérieur sont configurés. Le groupe de ponts 1 est à l'intérieur et le groupe de ponts 2 est une zone DMZ avec des serveurs Web publics. Les interfaces membres du groupe de ponts peuvent communiquer librement au sein du groupe de ponts, car chaque membre se trouve au même niveau de sécurité et nous avons activé la même

communication de sécurité. Bien que le niveau de sécurité du membre interne soit de 100 et que celui du membre de la zone DMZ soit également de 100, ces niveaux de sécurité ne s'appliquent pas aux communications inter-BVI; seuls les niveaux de sécurité BVI affectent le trafic inter-BVI. Les niveaux de sécurité des BVI et de l'extérieur (100, 50 et 0) autorisent implicitement le trafic de l'intérieur vers la zone DMZ et de l'intérieur vers l'extérieur; ainsi que de la zone DMZ vers l'extérieur. Un critère d'accès est appliqué à l'extérieur pour autoriser le trafic vers les serveurs de la zone DMZ.




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
```

```
!
interface gigabitethernet 1/5
  nameif dmz1
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
  service-object tcp destination eq smtp
!
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

Historique des interfaces en mode routé et en mode transparent

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Découverte de voisin IPv6	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les commandes suivantes : **ipv6 nd ns-interval**, **ipv6 nd ra-lifetime**, **ipv6 nd suppress-ra**, **ipv6 neighbor**, **ipv6 nd prefix**, **ipv6 nd dad-attempts**, **ipv6 nd reachable-time**, **ipv6 address**, **ipv6 enforce-eui64**.
Prise en charge d'IPv6 pour le mode transparent	8.2(1)	La prise en charge d'IPv6 a été introduite pour le mode de pare-feu transparent.
Groupes de ponts pour le mode transparent	v 8.4(1)	Si vous ne souhaitez pas le surdébit des contextes de sécurité ou si vous souhaitez optimiser votre utilisation des contextes de sécurité, vous pouvez regrouper les interfaces dans un groupe de ponts, puis configurer plusieurs groupes de ponts, un pour chaque réseau. Le trafic de groupe de ponts est isolé des autres groupes de ponts. Vous pouvez configurer jusqu'à huit groupes de ponts de quatre interfaces chacun en mode unique ou par contexte. Nous avons introduit les commandes suivantes : **interface bvi**, **show bridge-group**
Indicateurs de configuration d'adresse pour le relais DHCP IPv6	9.0(1)	Nous avons introduit les commandes suivantes : **ipv6 nd managed-config-flag**, **ipv6 nd other-config-flag**.
Nombre maximum de groupes de ponts en mode transparent augmenté à 250	9.3(1)	Le nombre maximum de groupes de ponts est passé de 8 à 250 groupes de ponts. Vous pouvez configurer jusqu'à 250 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces maximum par groupe de ponts. Nous avons modifié les commandes suivantes : **interface bvi**, **bridge-group**
Nombre maximum d'interfaces en mode transparent par groupe de ponts augmenté à 64	9.6(2)	Le nombre maximum d'interfaces par groupe de ponts est passé de 4 à 64. Nous n'avons pas modifié de commandes.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
DHCP IPv6	9.6(2)	L'ASA prend désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 : • Client d'adresse DHCPv6 : l'ASA obtient une adresse globale IPv6 et une route par défaut facultative du serveur DHCPv6. • Client de délégation de préfixe DHCPv6 : l'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. • Annonce de routeur BGP pour les préfixes délégués • Serveur sans état DHCPv6 : l'ASA fournit d'autres renseignements tels que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresses aux clients. Nous avons ajouté ou modifié les commandes suivantes : **clear ipv6 dhcp statistics, domain-name, dns-server, import, ipv6 address autoconfig, ipv6 address dhcp, ipv6 dhcp client pd, ipv6 dhcp client pd hint, ipv6 dhcp pool, ipv6 dhcp server, network, nis address, nis domain-name, nisp address, nisp domain-name, show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix, sip address, sip domain-name, sntp address**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage et pont intégrés	9.7(1)	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que l'ASA relie par des ponts au lieu de routes. L'ASA n'est pas un vrai pont, car l'ASA continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur l'ASA à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : mode de contexte multiple, mise en grappe d'ASA. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Nous avons modifié les commandes suivantes : **access-group, access-list ethertype, arp-inspection, dhcpd, mac-address-table static, mac-address-table aging-time, mac-learn, route, show arp-inspection, show bridge-group, show mac-address-table, show mac-learn**
Masque de sous-réseau 31 bits	9.7(1)	Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, la liaison de basculement entre 2 ASA ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog. Cette fonctionnalité n'est pas prise en charge pour les BVI pour les groupes de ponts ou avec le routage de multidiffusion. Nous avons modifié les commandes suivantes : **ip address, http, logging host, snmp-server, ssh**



CHAPITRE 21

Configuration avancée de l'interface

Ce chapitre décrit comment configurer les adresses MAC pour les interfaces, définir l'unité de transfert maximale (MTU), définir la taille de segment maximum TCP (TCP MSS) et autoriser une communication de même niveau de sécurité. La définition de la bonne MTU et de la taille de segment maximum TCP est essentielle pour garantir les meilleures performances du réseau.

- À propos des configurations avancées de l'interface, à la page 803
- Configurer manuellement l'adresse MAC, à la page 807
- Attribuer automatiquement des adresses MAC, à la page 808
- Configurer , la et le TCP MSS, à la page 809
- Autoriser la communication de niveau de sécurité identique, à la page 811
- Historique de la configuration avancée de l'interface, à la page 811

À propos des configurations avancées de l'interface

Cette section décrit les paramètres d'interface avancés.

À propos des adresses MAC

Vous pouvez affecter manuellement des adresses MAC pour remplacer la valeur par défaut. Pour le mode de contexte multiple, vous pouvez générer automatiquement des adresses MAC uniques (pour toutes les interfaces affectées à un contexte) et un mode de contexte unique (pour les sous-interfaces)..

Remarque Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de liaison IPv6 sont générées sur la base de l'adresse MAC, l'attribution d'adresses MAC uniques aux sous-interfaces permet d'obtenir des adresses locales de liaison IPv6 uniques, ce qui peut éviter la perturbation du trafic dans certaines instances du périphérique ASA.

Adresses MAC par défaut

Les attributions d'adresses MAC par défaut dépendent du type d'interface.

- Interfaces physiques : l'interface physique utilise l'adresse MAC gravée.

- Interfaces VLAN (Firepower 1010) —Mode de pare-feu routé : toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez Configurer manuellement l'adresse MAC, à la page 807

  Mode pare-feu transparent : chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez Configurer manuellement l'adresse MAC, à la page 807.

- EtherChannels (modèles Firepower) : pour un EtherChannel, toutes les interfaces qui font partie du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels. L'interface du canal de port utilise une adresse MAC unique provenant d'un pool; L'appartenance à l'interface n'affecte pas l'adresse MAC.

- EtherChannels (modèles ASA) : l'interface du canal de port utilise l'adresse MAC d'interface de groupe de canaux du plus petit numéro comme adresse MAC du canal de port. Vous pouvez aussi configurer une adresse MAC pour l'interface du canal de port. Nous vous recommandons de configurer une adresse MAC unique au cas où l'appartenance à l'interface du canal de groupe changerait. Si vous supprimez l'interface qui fournissait l'adresse MAC du canal de port, l'adresse MAC du canal de port passe à l'interface ayant le numéro le plus bas, ce qui perturbe le trafic.

- Sous-interfaces : toutes les sous-interfaces d'une interface physique utilisent la même adresse MAC gravée. Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur ASA.

Adresses MAC automatiques

En mode de contexte multiple, la génération automatique affecte des adresses MAC uniques à toutes les interfaces affectées à un contexte.

Si vous attribuez manuellement une adresse MAC et activez la génération automatique, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée, si elle est activée.

Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC pour l'interface.

Comme les adresses générées automatiquement (lors de l'utilisation d'un préfixe) commencent par A2, vous ne pouvez pas commencer les adresses MAC manuelles par A2 si vous souhaitez également utiliser la génération automatique.

Le châssis génère l'adresse MAC en utilisant le format suivant :

A2*xx.yyzz.zzzz*

Où *xx.yy* est un préfixe défini par l'utilisateur ou un préfixe généré automatiquement en fonction des deux derniers octets de l'adresse MAC de l'interface, et *zz.zzzz* est un compteur interne généré par l'ASA. Pour l'adresse MAC de secours, l'adresse est identique, sauf que le compteur interne est augmenté de 1.

Pour donner un exemple d'utilisation du préfixe, si vous définissez le préfixe 77, l'ASA convertit 77 en valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native de l'ASA :

A2**4D.00***zz.zzzz*

Pour un préfixe 1009 (03F1), l'adresse MAC est :

A2**F1.03***zz.zzzz*

Remarque Le format d'adresse MAC sans préfixe est une version existante. Consultez la commande **mac-address auto** dans la référence de commandes pour plus d'informations sur le format existant.

À propos de la MTU

La MTU spécifie la taille maximale de la *charge utile* de trame que l'ASA peut transmettre sur une interface Ethernet donnée. La valeur MTU correspond à la taille de la trame *sans* en-tête Ethernet, sans balisage VLAN ou autre surdébit. Par exemple, lorsque vous définissez la MTU sur 1500, la taille de trame attendue est de 1518 octets, en-têtes compris, ou de 1522 lorsque vous utilisez le VLAN. Ne définissez pas la valeur MTU plus élevée pour prendre en charge ces en-têtes.

Pour VXLAN ou Geneve, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet IP est plus volumineux et nécessite une MTU plus grande : vous devez définir la MTU de l'interface source VTEP ASA sur la MTU du réseau + 54 octets (pour VXLAN) ou + 306 octets (Genève).

Chemin de découverte de MTU

L'ASA prend en charge la découverte de chemin MTU (comme défini dans la RFC 1191), qui permet à tous les périphériques d'un chemin réseau entre deux hôtes de coordonner la MTU afin qu'ils puissent normaliser sur la MTU la plus basse du chemin.

MTU par défaut

Par défaut, la MTU sur ASA est de 1500 octets. Cette valeur n'inclut pas les 18 à 22octets pour l'en-tête Ethernet, le balisage VLAN ou d'autres surdébits.

Lorsque vous activez VXLAN sur l'interface source VTEP, si la MTU est inférieure à 1 554 octets, l'ASA l'augmente automatiquement à 1 554 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. En général, vous devez définir la MTU de l'interface source de l'ASA comme étant la MTU du réseau + 54 octets.

MTU et fragmentation.

Pour IPv4, si un paquet IP sortant dépasse la MTU spécifiée, il est fragmenté en au moins deux trames. Les fragments sont réassemblés à la destination (et parfois aux sauts intermédiaires), et la fragmentation peut dégrader les performances. Pour IPv6, la fragmentation des paquets n'est généralement pas autorisée. Par conséquent, vos paquets IP doivent respecter la taille de la MTU pour éviter la fragmentation.

Pour les paquets TCP, les points terminaux utilisent généralement leur MTU pour déterminer la taille maximale du segment TCP (MTU – 40, par exemple). Si des en-têtes TCP supplémentaires sont ajoutés en cours de route, par exemple pour les tunnels VPN de site à site, le MSS TCP devra peut-être être ajusté par l'entité de tunnellisation. Consultez À propos de TCP MSS, à la page 806.

Pour UDP ou ICMP, l'application doit prendre en compte la MTU pour éviter la fragmentation.

Remarque L'ASA peut recevoir des trames plus grandes que la MTU configurée tant qu'il y a de l'espace en mémoire.

MTU et trames grand format

Une MTU plus grande vous permet d'envoyer des paquets plus volumineux. Des paquets plus volumineux pourraient être plus efficaces pour votre réseau. Consultez les consignes suivantes :

- Correspondance des MTU sur le chemin de trafic : nous vous recommandons de définir la MTU sur toutes les interfaces ASA et les autres interfaces de périphériques le long du chemin de trafic. La correspondance des MTU empêche les périphériques intermédiaires de fragmenter les paquets.
- Prise en charge des trames étendues : vous pouvez définir la MTU à 9 000 octets ou plus lorsque vous activez les trames étendues. Le maximum dépend du modèle.

À propos de TCP MSS

La taille maximale de segment (MSS) TCP est la taille de la charge utile TCP *avant* l'ajout des en-têtes TCP et IP. Les paquets UDP ne sont pas concernés. Le client et le serveur échangent des valeurs TCP MSS lors de la prise de contact tridirectionnelle lors de l'établissement de la connexion.

Vous pouvez définir le MSS TCP sur l'ASA pour le trafic de transit; par défaut, le MSS TCP maximal est défini sur 1380 octets. Ce paramètre est utile lorsque ASA doit augmenter la taille du paquet pour l'encapsulation VPN IPsec. Cependant, pour les points terminaux non IPsec, vous devez désactiver le MSS TCP maximal sur ASA.

Si vous définissez un MSS TCP maximal, si l'une ou l'autre des extrémités d'une connexion demande un MSS TCP supérieur à la valeur définie sur l'ASA, alors l'ASA remplace le MSS TCP dans le paquet de demande par l'ASA maximum. Si l'hôte ou le serveur ne demande pas de message MSS du protocole TCP, ASA assume la valeur par défaut de la RFC 793 de 536 octets (IPv4) ou de 1 220 octets (IPv6), mais ne modifie pas le paquet. Par exemple, vous laissez la MTU par défaut à 1500 octets. Un hôte demande un MSS de 1500 moins la longueur de l'en-tête TCP et IP, ce qui définit le MSS à 1460. Si le MSS TCP maximal de l'ASA est de 1 380 (par défaut), l'ASA modifie la valeur du MSS dans le paquet de demande TCP à 1380. Le serveur envoie ensuite des paquets avec une charge utile de 1380 octets. L'ASA peut alors ajouter jusqu'à 120 octets d'en-tête au paquet tout en conservant la taille de MTU de 1500.

Vous pouvez également configurer le MSS TCP minimal; si un hôte ou un serveur demande un très petit MSS TCP, ASA peut augmenter la valeur. Par défaut, le MSS TCP minimal n'est pas activé.

Pour le trafic vers la boîte, y compris pour les connexions SSL VPN, ce paramètre ne s'applique pas. L'ASA utilise la MTU pour calculer le TCP MSS : MTU – 40 (IPv4) ou MTU – 60 (IPv6).

TCP MSS par défaut

Par défaut, le MSS TCP maximal sur l'ASA est de 1380 octets. Cette valeur par défaut convient aux connexions VPN IPsec IPv4 où la valeur des en-têtes peut atteindre 120 octets; Cette valeur correspond à la MTU par défaut de 1500 octets.

Paramètre MSS TCP maximal suggéré

Le MSS TCP par défaut suppose que l'ASA agit comme un point terminal de VPN IPsec IPv4 et a une MTU de 1500. Lorsque l'ASA agit comme un point terminal de VPN IPsec IPv4, il doit gérer jusqu'à 120 octets pour les en-têtes TCP et IP.

Si vous modifiez la valeur MTU, utilisez IPv6 ou n'utilisez pas ASA comme point terminal VPN IPsec, vous devez modifier le paramètre TCP MSS.

Consultez les consignes suivantes :

- Normal Traffic (Trafic normal) : Désactivez la limite TCP MSS et acceptez la valeur établie entre les points terminaux de connexion. Étant donné que les points terminaux de connexion dérivent généralement le MSS TCP de la MTU, les paquets non IPsec correspondent généralement à ce MSS TCP.
- IPv4 IPsec endpoint traffic : Définissez le MSS TCP maximal sur la MTU - 120. Par exemple, si vous utilisez des trames étendues et que vous définissez la MTU à 9000, vous devez définir le MSS TCP sur 8880 pour profiter de la nouvelle MTU.
- IPv6 IPsec endpoint Traffic (Trafic de point terminal IPsec IPv6) : définissez le MSS TCP maximal sur la MTU - 140.

Communication inter-interface

Permettre à des interfaces de même niveau de sécurité de communiquer entre elles offre les avantages suivants :

- Vous pouvez configurer plus de 101 interfaces de communication.

  Si vous utilisez différents niveaux pour chaque interface et n'affectez aucune interface au même niveau de sécurité, vous ne pouvez configurer qu'une seule interface par niveau (de 0 à 100).

- Vous souhaitez que le trafic passe librement entre toutes les mêmes interfaces de sécurité sans ACL.

Si vous activez la même communication d'interface de sécurité, vous pouvez toujours configurer des interfaces à différents niveaux de sécurité, comme d'habitude.

Communication intra-interface (mode de pare-feu routé)

La communication intra-interface peut être utile pour le trafic VPN qui entre dans une interface, mais qui est ensuite acheminé vers la même interface. Dans ce cas, le trafic VPN peut être non chiffré ou rechiffré pour une autre connexion VPN. Par exemple, si vous avez un réseau VPN en étoile, où l'ASA est le concentrateur et les réseaux VPN distants sont des rayons, pour qu'un rayon communique avec un autre rayon, le trafic doit entrer dans l'ASA, puis ressortir vers l'autre rayon.



Remarque Tout le trafic autorisé par cette fonctionnalité reste soumis aux règles du pare-feu. Veillez à ne pas créer de situation de routage asymétrique qui pourrait empêcher le trafic de retour de traverser l'ASA.

Configurer manuellement l'adresse MAC

Si vous devez attribuer manuellement l'adresse MAC, vous pouvez le faire en suivant cette procédure.

Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur ASA.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *id*

Exemple :

```
ciscoasa(config)# interface gigabithethernet 0/0
```

Étape 2 Attribuez une adresse MAC privée à cette interface :

mac-address *mac_address* [**standby** *mac_address*]

Exemple :

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

La *mac_address* est au format H.H.H., où H est une valeur hexadécimale de 16 bits. Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE est saisie comme suit : 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.

Les deux premiers octets d'une adresse MAC manuelle ne peuvent pas être A2 si vous souhaitez également utiliser des adresses MAC générées automatiquement.

Pour une utilisation avec le basculement, définissez l'adresse MAC en veille (**standby**). Si l'unité active bascule et que l'unité en veille devient active, la nouvelle unité active commence à utiliser les adresses MAC actives pour minimiser les perturbations du réseau, tandis que l'ancienne unité active utilise l'adresse en veille.

Attribuer automatiquement des adresses MAC

Cette section décrit comment configurer la génération automatique des adresses MAC. Pour le mode de contexte multiple, cette fonctionnalité attribue des adresses MAC uniques à tous les types d'interfaces qui sont affectés à un contexte. Pour le mode de contexte unique, cette fonctionnalité attribue des adresses MAC uniques aux sous-interfaces VLAN.

Avant de commencer

- Lorsque vous configurez une commande **nameif** pour l'interface, la nouvelle adresse MAC est générée immédiatement. Si vous activez cette fonctionnalité après avoir configuré les interfaces, les adresses MAC sont générées pour toutes les interfaces immédiatement après leur activation. Si vous désactivez cette fonctionnalité, l'adresse MAC par défaut de chaque interface revient à l'adresse MAC. Par exemple, les sous-interfaces de GigabitEthernet 0/1 utilisent l'adresse MAC de GigabitEthernet 0/1.
- Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC pour l'interface.
- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Attribuez automatiquement des adresses MAC privées à chaque interface :

mac-address auto [**prefix** *prefix*]

Si vous n'écrivez pas de préfixe, l'ASA génère automatiquement ce dernier en fonction des deux derniers octets de l'adresse MAC de l'interface.

Si vous saisissez manuellement un préfixe, le *préfixe* est une valeur décimale comprise entre 0 et 65 535. Ce préfixe est converti en nombre hexadécimal à quatre chiffres et utilisé dans l'adresse MAC.

Exemple :

```
ciscoasa(config)# mac-address auto prefix 19
```

Configurer , la et le TCP MSS

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.
- Pour augmenter la MTU au-dessus de 1500, activez les trames étendues selon Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 678.

Procédure

Étape 1 Définissez la MTU. Le minimum et le maximum dépendent de votre plateforme.

mtu *interface_name bytes*

Exemple :

```
ciscoasa(config-if)# mtu inside ?

configure mode commands/options:
  <64-9198>  MTU bytes
ciscoasa(config)# mtu inside 9000
```

Par défaut, la MTU est de 1500 octets.

Remarque
Lorsque vous définissez le MTU pour une interface ou de canal de port, l'ASA applique le paramètre à toutes les interfaces membres.

Pour certains modèles qui prennent en charge les bâtis grand format, si vous entrez une valeur supérieure à 1500 pour une interface, vous devez activer la prise en charge des bâtis grand format. Consultez Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 678.

Étape 2 Configurez la taille de segment TCP maximale en octets, entre 48 et tout nombre maximal :

sysopt connection tcpmss [**minimum**] *bytes*

Exemple :

```
ciscoasa(config)# sysopt connection tcpmss 8500
ciscoasa(config)# sysopt connection tcpmss minimum 1290
```

Par défaut, la MTU est de 1380 octets. Vous pouvez désactiver cette fonctionnalité en mettant les octets à **0**.

Pour le mot clé **minimum**, définit la taille de segment maximale pour qu'elle ne soit pas inférieure à *octets* (entre 48 et 65 535). La fonctionnalité minimale est désactivée par défaut (définie sur 0).

Étape 3 Configurez le nombre maximal de segments TCP non traités.

sysopt connection tcp-max-unprocessed-seg *segments non traités*

Exemple :

```
ciscoasa(config)# sysopt connection tcp-max-unprocessed-seg 7
```

La valeur par défaut est 6. La valeur doit être comprise entre 6 et 24.

Exemples

Dans l’exemple suivant, les trames étendues sont activées, la MTU est augmentée sur toutes les interfaces et TCP MSS est désactivé pour le trafic en dehors de VPN (en définissant TCP MSS sur 0, ce qui signifie qu’il n’y a pas de limite) :

```
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 0
```

Dans l'exemple suivant, les trames étendues sont activées, la MTU est augmentée sur toutes les interfaces et TCP MSS est modifié pour le trafic VPN à 9078 (la MTU moins 120) :

```
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

Autoriser la communication de niveau de sécurité identique

Par défaut, les interfaces de même niveau de sécurité ne peuvent pas communiquer entre elles, et les paquets ne peuvent pas entrer ni sortir de la même interface. Cette section décrit comment activer la communication inter-interfaces lorsque les interfaces se trouvent sur le même niveau de sécurité et comment activer la communication intra-interface.

Procédure

Étape 1 Activez les interfaces sur le même niveau de sécurité afin qu'elles puissent communiquer entre elles :

same-security-traffic permit inter-interface

Étape 2 Activez la communication entre les hôtes connectés à la même interface :

same-security-traffic permit intra-interface

Historique de la configuration avancée de l'interface

Tableau 31 : Historique de la configuration avancée de l'interface

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
La MTU maximale est maintenant de 9 198 octets.	9.1(6), 9.2(1)	La MTU maximale que l'ASA peut utiliser est de 9 198 octets (vérifiez la limite exacte de votre modèle à l'aide de l'interface de ligne de commande). Cette valeur n'inclut pas l'en-tête de couche 2. L'ASA vous a permis de définir une MTU maximale de 65 535 octets, ce qui était inexact et pourrait causer des problèmes. Si votre MTU a été définie à une valeur supérieure à 9 198, la MTU est automatiquement réduite lors de la mise à niveau. Dans certains cas, cette modification de la MTU peut entraîner une non-concordance de la MTU. Assurez-vous de configurer tout équipement de connexion pour utiliser la nouvelle valeur MTU. Nous avons modifié la commande suivante : **mtu**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Augmentation de la taille de la MTU pour l'ASA sur le Châssis Firepower 4100/9300	9.6(2)	Vous pouvez définir la MTU maximale à 9 184 octets sur les périphériques Firepower 4100 et 9300; auparavant, le maximum était de 9 000 octets. Cette MTU est prise en charge par FXOS 2.0.1.68 et les versions ultérieures. Nous avons modifié la commande suivante : **mtu**
Génération d'adresses MAC uniques en mode de contexte unique	9.8(3), 9.8(4), 9.9(2)	Vous pouvez maintenant activer la génération d'adresses MAC uniques pour les sous-interfaces VLAN en mode de contexte unique. Normalement, les sous-interfaces partagent la même adresse MAC avec l'interface principale. Comme les adresses Link-Local IPv6 sont générées en fonction de l'adresse MAC, cette fonctionnalité permet d'utiliser des adresses Link-Local IPv6 uniques. Commande nouvelle ou modifiée : **mac-address auto**
La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée pour les interfaces de 1 Gigabit et les versions ultérieures.	9.17(1)	La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée pour les interfaces de 1 Gigabit et les versions ultérieures. Pour les autres modèles de ports SFP, l'option **no speed nonegotiate** définit la vitesse à 1 000 Mbit/s; la nouvelle commande signifie que vous pouvez définir la négociation automatique et la vitesse indépendamment. Commandes nouvelles ou modifiées : **negotiate-auto**



CHAPITRE 22

Zones de circulation

Vous pouvez attribuer plusieurs interfaces à une *zone de trafic*, ce qui permet au trafic d'un flux existant de sortir ou d'entrer dans l'ASA sur n'importe quelle interface de la zone. Cette fonctionnalité permet le routage à chemins multiples à coûts égaux (ECMP) sur l'ASA, ainsi qu'à équilibrer la charge externe du trafic vers l'ASA sur plusieurs interfaces.

- À propos des zones de trafic, à la page 813
- Conditions préalables aux zones de trafic, à la page 819
- Lignes directrices relatives aux zones de trafic, à la page 821
- Configurer une zone de trafic, à la page 822
- Supervision des zones de trafic, à la page 823
- Exemple de zones de trafic, à la page 825
- Historique des zones de trafic, à la page 828

À propos des zones de trafic

Cette section décrit comment vous devez utiliser les zones de trafic dans votre réseau.

Comportement non zoné

L'algorithme de sécurité adaptatif prend en compte l'état d'un paquet lorsqu'il décide d'autoriser ou de refuser le trafic. L'un des paramètres appliqués pour le flux est que le trafic entre et sort de la même interface. Tout trafic pour un flux existant qui entre dans une interface différente est abandonné par l'ASA.

Les zones de trafic vous permettent de regrouper plusieurs interfaces afin que le trafic entrant ou sortant de *n'importe* quelle interface de la zone soit soumis aux contrôles de sécurité de l'algorithme de sécurité adaptatif.

Sujets connexes

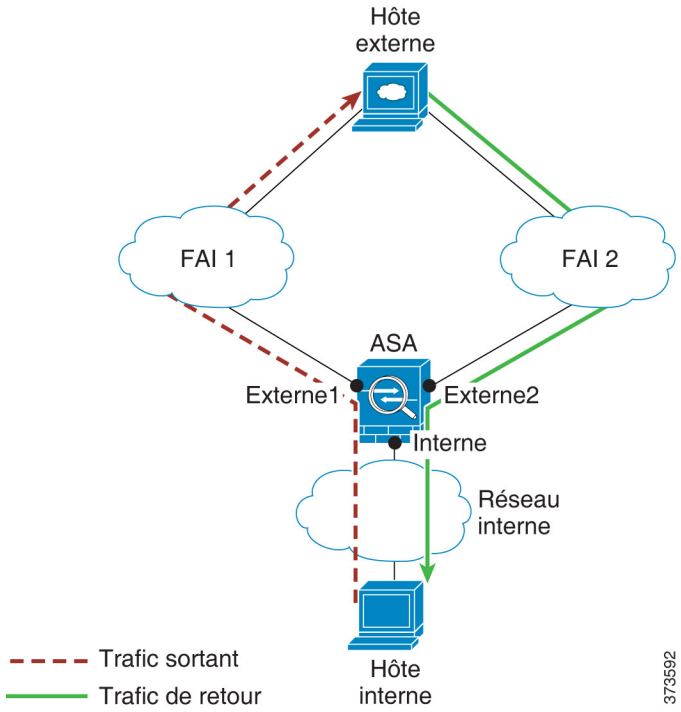
Présentation de l'inspection dynamique, à la page 7

Pourquoi utiliser des zones?

Vous pouvez utiliser des zones pour vous servir de plusieurs scénarios de routage.

Routage asymétrique

Dans le scénario suivant, une connexion a été établie entre un hôte interne et un hôte externe par le biais du FAI 1 sur l'interface Externe1. En raison d'un routage asymétrique sur le réseau de destination, le trafic de retour est arrivé du FAI 2 sur l'interface Externe2.

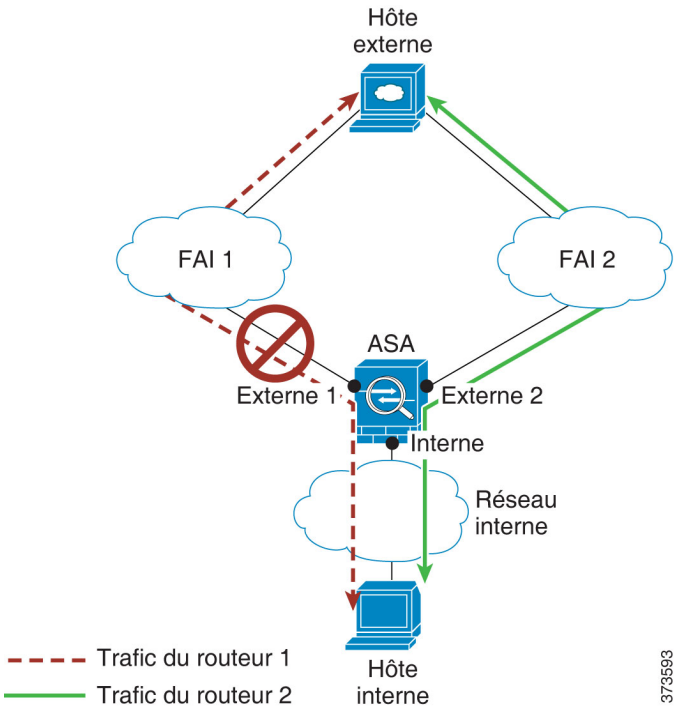


Problème non zoné : l'ASA gère les tables de connexion par interface. Lorsque le trafic de retour arrivera à Externe2, il ne correspondra pas à la table de connexion et sera abandonné. Pour une grappe ASA, le routage asymétrique lorsque la grappe a plusieurs contiguïtés avec le même routeur peut entraîner une perte de trafic inacceptable.

Solution zonée : l'ASA gère les tables de connexion par zone. Si vous regroupez Externe1 et Externe2 dans une zone, lorsque le trafic de retour arrivera à Externe2, il correspondra à la table de connexion par zone et la connexion sera autorisée.

Route perdue

Dans le scénario suivant, une connexion a été établie entre un hôte interne et un hôte externe par le biais du FAI 1 sur l'interface Externe1. En raison d'une route perdue ou déplacée entre Externe1 et le FAI 1, le trafic doit emprunter une route différente par le FAI 2.

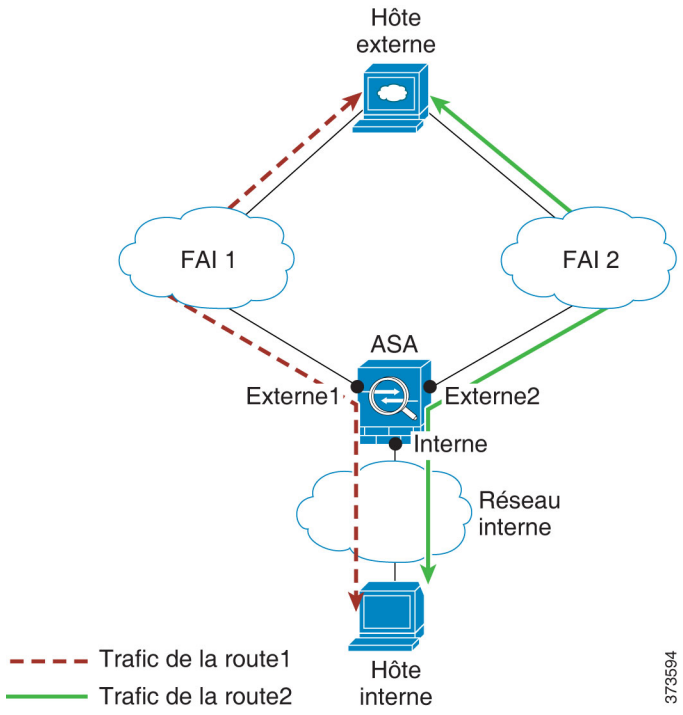


Problème non zoné : la connexion entre les hôtes interne et externe sera supprimée; une nouvelle connexion doit être établie à l'aide d'une nouvelle route optimale. Pour UDP, la nouvelle route sera utilisée après un seul abandon de paquet, mais pour TCP, une nouvelle connexion doit être rétablie.

Solution zonée : l'ASA détecte la route perdue et commute le flux dans le nouveau chemin par le biais du FAI 2. Le trafic sera transféré de manière transparente sans aucun abandon de paquets.

Équilibrage de la charge

Dans le scénario suivant, une connexion a été établie entre un hôte interne et un hôte externe par le biais du FAI 1 sur l'interface Externe1. Une deuxième connexion a été établie par le biais d'une route à coût égal par le biais du FAI 2 sur l'interface Externe2.



Problème non zoné : l'équilibrage de charges sur les interfaces n'est pas possible; vous ne pouvez équilibrer la charge qu'avec des routes à coût égal sur une interface.

Solution zonée : l'ASA équilibre les connexions sur un maximum de huit routes à coût égal sur toutes les interfaces de la zone.

Tables de connexion et de routage par zone

L'ASA gère une table de connexion par zone afin que le trafic puisse arriver sur n'importe quelle interface de zone. L'ASA gère également une table de routage par zone pour la prise en charge ECMP.

Routage ECMP

L'ASA prend en charge le routage à chemins multiples à coûts égaux (ECMP).

Prise en charge ECMP non zonée

Sans zones, vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal par interface. Par exemple, vous pouvez configurer trois routes par défaut sur l'interface externe qui spécifient différentes passerelles :

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

Dans ce cas, le trafic est équilibré en charge sur l'interface externe entre 10.1.1.2, 10.1.1.3 et 10.1.1.4. Le trafic est réparti entre les passerelles précisées selon un algorithme qui procède au hachage des adresses IP source et de destination, de l'interface entrante, du protocole et des ports source et destination.

Le protocole ECMP n'est pas pris en charge sur plusieurs interfaces; vous ne pouvez donc pas définir de route vers la même destination sur une interface différente. La route suivante n'est pas autorisée lorsqu'elle est configurée avec l'une des routes ci-dessus :

```
route outside2 0 0 10.2.1.1
```

Prise en charge ECMP zonée

Avec les zones, vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal sur 8 interfaces au maximum dans une zone. Par exemple, vous pouvez configurer trois routes par défaut sur trois interfaces dans la zone :

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

De même, votre protocole de routage dynamique peut configurer automatiquement des routes à coût égal. L'ASA équilibre la charge du trafic entre les interfaces grâce à un mécanisme d'équilibrage de la charge plus robuste.

Lorsqu'un routage est perdu, l'ASA déplace le flux de manière transparente vers une autre route.

Équilibrage de charges des connexions

L'ASA équilibre la charge des connexions sur des routes à coût égal à l'aide d'un hachage effectué à partir du paquet à six tuples (adresses IP source et de destination, port de destination, protocole et interface d'entrée). À moins que la route ne soit perdue, une connexion restera sur l'interface choisie pendant sa durée.

Les paquets d'une connexion ne sont pas équilibrés en charge sur toutes les routes; une connexion utilise une seule route, sauf si cette route est perdue.

L'ASA ne prend pas en compte la bande passante de l'interface ni d'autres paramètres lors de l'équilibrage de charges. Vous devez vous assurer que toutes les interfaces de la même zone ont les mêmes caractéristiques telles que la MTU, la bande passante, etc.

L'algorithme d'équilibrage de charges n'est pas configurable par l'utilisateur.

Basculement vers une route dans une autre zone

Lorsqu'une route est perdue sur une interface, s'il n'y a aucune autre route disponible dans la zone, l'ASA utilisera une route d'une interface ou d'une zone différente. Si cette route de secours est utilisée, vous pouvez rencontrer des abandons de paquet comme avec la prise en charge du routage non zoné.

Politique de sécurité basée sur l'interface

Les zones permettent le trafic vers et en provenance de n'importe quelle interface de la zone, mais la politique de sécurité elle-même (critères d'accès, NAT, etc.) est toujours appliquée par interface et non par zone. Si vous configurez la même politique de sécurité pour toutes les interfaces de la zone, vous pouvez alors mettre en œuvre avec succès l'ECMP et l'équilibrage de charges pour ce trafic. Pour en savoir plus sur la configuration d'interface parallèle requise, consultez Conditions préalables aux zones de trafic, à la page 819.

Services pris en charge pour les zones de trafic

Les services suivants sont pris en charge avec les zones :

- Règles d'accès
- NAT
- Règles de service, à l'exception du contrôle de trafic QoS.
- Routage

Vous pouvez également configurer les services vers et à partir de la boîte répertoriés dans Trafic entrant et sortant, à la page 819, bien que la prise en charge complète des zones ne soit pas disponible.

Ne configurez pas d'autres services (comme le VPN ou le filtre de trafic de réseau de zombies) pour les interfaces dans une zone de trafic; elles peuvent ne pas fonctionner ou évoluer comme prévu.

Remarque Pour obtenir des renseignements détaillés sur la configuration de la politique de sécurité, consultez Conditions préalables aux zones de trafic, à la page 819.

Niveaux de sécurité

La première interface que vous ajoutez à une zone détermine le niveau de sécurité de la zone. Toutes les interfaces supplémentaires doivent avoir le même niveau de sécurité. Pour modifier le niveau de sécurité des interfaces d'une zone, vous devez supprimer toutes les interfaces sauf une, puis modifier les niveaux de sécurité et rajouter les interfaces.

Interface principale et actuelle pour le flux

Chaque flux de connexion est créé en fonction des interfaces d'entrée et de sortie initiales. Ces interfaces sont les interfaces *principales*.

Si une nouvelle interface de sortie est utilisée en raison de modifications de routes ou d'un routage asymétrique, les nouvelles interfaces sont les interfaces *actuelles*.

Rejoindre ou quitter une zone

Lorsque vous affectez une interface à une zone, toutes les connexions sur cette interface sont supprimées. Les connexions doivent être rétablies.

Si vous supprimez une interface d'une zone, toutes les connexions qui ont l'interface comme interface principale sont supprimées. Les connexions doivent être rétablies. Si l'interface est l'interface actuelle, l'ASA ramène les connexions à l'interface principale. La table de routage de zone est également actualisée.

Trafic intra-zone

Pour permettre au trafic d'*entrer* dans une interface et d'en *sortir*par une autre dans la même zone, activez la commande **same-security permit intra-interface**, qui permet au trafic d'entrer et de sortir de la même

interface, ainsi que la commande **same-security permit inter-interface**, qui autorise le trafic entre les interfaces de même sécurité. Sinon, un flux ne peut pas être acheminé entre deux interfaces dans la même zone.

Trafic entrant et sortant

- Vous ne pouvez pas ajouter des interfaces de gestion uniquement ou d'accès de gestion à une zone.
- Pour le trafic de gestion sur les interfaces régulières d'une zone, seul le routage asymétrique sur les flux existants est pris en charge; il n'y a pas de prise en charge ECMP.
- Vous ne pouvez configurer un service de gestion que sur une seule interface de zone, mais pour profiter de la prise en charge du routage asymétrique, vous devez le configurer sur toutes les interfaces. Même lorsque les configurations sont parallèles sur toutes les interfaces, ECMP n'est pas pris en charge.
- L'ASA prend en charge les services entrant et sortant suivants dans une zone :
  - Telnet
  - SSH
  - HTTPS
  - SNMP
  - Journal système

Chevauchement d'adresses IP dans une zone

Pour les interfaces non zonées, l'ASA prend en charge les réseaux d'adresses IP qui se chevauchent sur les interfaces tant que vous configurez la NAT correctement. Cependant, les réseaux qui se chevauchent ne sont pas pris en charge sur les interfaces de la même zone.

Conditions préalables aux zones de trafic

- Configurez tous les paramètres d'interface, y compris le nom, l'adresse IP et le niveau de sécurité. Notez que le niveau de sécurité doit correspondre pour toutes les interfaces de la zone. Il est conseillé de regrouper les interfaces similaires en termes de bande passante et d'autres propriétés de couche 2.
- Configurez les services suivants pour qu'ils correspondent sur toutes les interfaces de zone :
  - Critères d'accès : appliquez le même critère d'accès à toutes les interfaces membres de la zone ou utilisez un critère d'accès global.

    Par exemple :

```
access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
access-group ZONE1 in interface outside1
access-group ZONE1 in interface outside2
access-group ZONE1 in interface outside3
```

- NAT : configurez la même politique NAT sur toutes les interfaces membres de la zone ou utilisez une règle NAT globale (en d'autres termes, utilisez « any » pour représenter les interfaces dans la règle NAT).

  L'interface PAT n'est pas prise en charge.

  Par exemple :

```
object network WEBSERVER1
  host 10.9.9.9 255.255.255.255
  nat (inside,any) static 209.165.201.9
```



Remarque Lorsque vous utilisez des ensembles NAT et PAT spécifiques à l'interface, l'ASA ne peut pas commuter les connexions en cas de défaillance de l'interface d'origine.

Si vous utilisez des ensembles PAT spécifiques à l'interface, plusieurs connexions du même hôte peuvent équilibrer la charge vers différentes interfaces et utiliser différentes adresses IP mappées. Les services Internet qui utilisent plusieurs connexions simultanées peuvent ne pas fonctionner correctement dans ce cas.

- Règles de service : utilisez la politique de service globale ou attribuez la même politique à chaque interface d'une zone.

  Le contrôle de trafic QoS n'est pas pris en charge.

  Par exemple :

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```



Remarque Pour les inspections VoIP, l'équilibrage de charges de la zone peut entraîner une augmentation des paquets désordonnés. Cette situation peut se produire, car les paquets ultérieurs peuvent atteindre l'ASA avant les paquets antérieurs qui empruntent un chemin différent. Les symptômes des paquets désordonnés sont les suivants :

  - Utilisez la mémoire plus élevée aux nœuds intermédiaires (pare-feu et IDS) et aux nœuds de réception de la file d'attente si la mise en file d'attente est utilisée.
  - Mauvaise qualité vidéo ou vocale.

  Pour maîtriser ces effets, nous vous conseillons d'utiliser les adresses IP uniquement pour la répartition de la charge pour le trafic VoIP.

- Configurez le routage en tenant compte des capacités de la zone ECMP.

Lignes directrices relatives aux zones de trafic

Mode pare-feu

Pris en charge uniquement en mode de pare-feu routé. Ne prend pas en charge le mode de pare-feu transparent ni les interfaces de groupe de ponts en mode routé.

Basculement

- Vous ne pouvez pas ajouter la liaison de basculement ou d'état à une zone.
- En mode de basculement actif/actif, vous pouvez attribuer une interface dans chaque contexte à un groupe de routage asymétrique (ASR). Ce service permet de restaurer le trafic renvoyé sur une interface similaire de l'unité homologue vers l'unité d'origine. Vous ne pouvez pas configurer à la fois des groupes ASR et des zones de trafic dans un contexte. Si vous configurez une zone dans un contexte, aucune des interfaces de contexte ne peut faire partie d'un groupe ASR. Consultez Configurer la prise en charge des paquets routés asymétriques (mode actif/actif), à la page 315 pour de plus amples renseignements sur les groupes ASR.
- Seules les interfaces principales de chaque connexion sont répliquées sur l'unité en veille; les interfaces actuelles ne sont pas répliquées. Si l'unité en veille devient active, elle attribuera une nouvelle interface actuelle, au besoin.

Mise en grappe

- Vous ne pouvez pas ajouter la liaison de commande de grappe à une zone.

Directives sur les modèles

Vous ne pouvez pas ajouter les ports de commutation ni les interfaces VLAN de Firepower 1010 à une zone.

Directives supplémentaires

- Vous pouvez créer un maximum de 256 zones.
- Vous pouvez ajouter les types d'interfaces suivants à une zone :
  - Physique
  - VLAN
  - EtherChannel
- Vous ne pouvez pas ajouter les types d'interfaces suivants :
  - Gestion uniquement
  - Accès de gestion
  - Liaison de basculement ou d'état
  - Liaison de commande de la grappe
  - Interfaces membres dans un EtherChannel

  - VNI; de plus, si une interface de données standard est marquée comme nve-only, elle ne peut pas être membre d'une zone.
  - BVI ou interfaces membres d'un groupe de ponts.

- Une interface ne peut être membre que d'une seule zone.
- Vous pouvez inclure jusqu'à 8 interfaces par zone.
- Pour ECMP, vous pouvez ajouter jusqu'à 8 routes à coût égal par zone, sur toutes les interfaces de zone. Vous pouvez également configurer plusieurs routes sur une seule interface dans le cadre de la limite de 8 routes.
- Lorsque vous ajoutez une interface à une zone, toutes les routes statiques de ces interfaces sont supprimées.
- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone de trafic.
- L'ASA ne prend pas en charge le réassemblage des paquets fragmentés pour les fragments dont la charge est équilibrée sur des interfaces distinctes; ces fragments seront abandonnés.
- Le routage de multidiffusion PIM/IGMP n'est pas pris en charge sur les interfaces dans une zone.

Configurer une zone de trafic

Configurez une zone nommée et affectez des interfaces à la zone.

Procédure

Étape 1 Ajouter la zone :

zone *name*

Exemple :

```
zone outside
```

Le nom de la zone peut comporter jusqu'à 48 caractères.

Étape 2 Ajoutez une interface à la zone :

interface *id* **zone-member** *zone_name*

Exemple :

```
interface gigabitethernet0/0
  zone-member outside
```

Étape 3 Ajoutez d'autres interfaces à la zone. assurez-vous qu'elles ont le même niveau de sécurité que la première interface que vous avez ajoutée.

Exemple :

```
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

Exemples

Dans l'exemple suivant, une zone externe est configurée avec quatre interfaces membres :

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

Supervision des zones de trafic

Cette section décrit comment superviser les zones de trafic.

Renseignements sur la zone

- **show zone** [*name*]

  Affiche l'ID de zone, le contexte, le niveau de sécurité et les membres.

  Consultez la sortie suivante pour la commande **show zone** :

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  Affiche les noms d'interface et les noms de zone.

  Consultez la sortie suivante pour la commande **show nameif zone** :

```
ciscoasa# show nameif zone
Interface               Name                    zone-name      Security
```

```
GigabitEthernet0/0       inside-1              inside-zone     100
GigabitEthernet0/1.21    inside                inside-zone     100
GigabitEthernet0/1.31    4                                       0
GigabitEthernet0/2       outside               outside-zone   0
Management0/0            lan                                     0
```

Connexions de zone

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

  La commande **show conn zone** affiche les connexions pour une zone. Les mots clés **long** et **detail** affichent l'interface principale sur laquelle la connexion a été établie, et celle entre parenthèses est l'interface actuellement utilisée pour transférer le trafic ou l'interface d'où provient le dernier paquet. Ainsi, l'interface actuelle, dans le cas d'une connexion provenant de plusieurs interfaces, peut afficher différentes interfaces à différents moments selon le moment où la commande show conn a été émise.

  Consultez la sortie suivante pour la commande **show conn long zone** :

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  Affiche les tableaux de chemin de sécurité accélérés à des fins de débogage.

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  Affiche les états du réseau des hôtes locaux dans une zone.

  Consultez la sortie suivante pour la commande **show local-host zone**. L'interface principale est répertoriée en premier et l'interface actuelle est entre parenthèses.

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
 TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

Routage de zone

- **show route zone**

  Affiche les routes pour les interfaces de zone.

  Consultez la sortie suivante pour la commande **show route zone** :

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

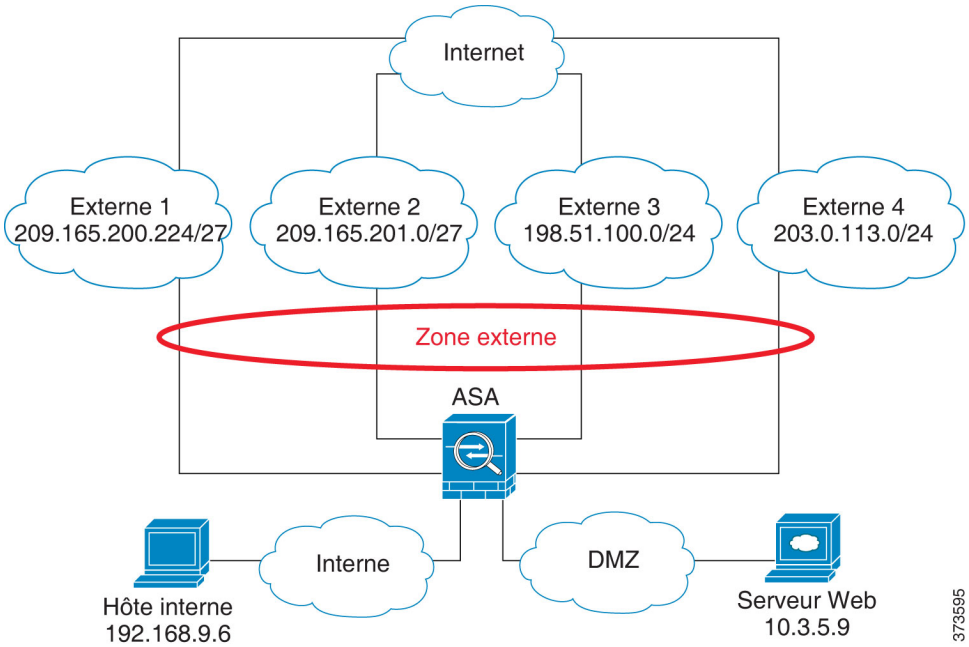
  Affiche les tableaux de chemins de sécurité accélérés à des fins de débogage et affiche la zone associée à chaque route.

  Consultez la sortie suivante pour la commande **show asp table routing** :

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67       255.255.255.255 mgmt
out  172.0.0.0        255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

Exemple de zones de trafic

L'exemple suivant affecte 4 interfaces VLAN à la zone externe et configure 4 routes par défaut à coût égal. La PAT est configurée pour l'interface interne, et un serveur Web est disponible sur une interface DMZ à l'aide de la NAT statique.




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown
```

```
interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
```

```
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

Historique des zones de trafic

Nom de la caractéristique	Versions de plateforme	Description
Zones de circulation	9.3(2)	Vous pouvez regrouper les interfaces dans une zone de trafic pour réaliser l'équilibrage de la charge de trafic (à l'aide du routage ECMP (chemins multiples à coût égal)), la redondance de routes et le routage asymétrique sur plusieurs interfaces. **Remarque** Vous ne pouvez pas appliquer de politique de sécurité à une zone nommée; la politique de sécurité est basée sur l'interface. Lorsque les interfaces d'une zone sont configurées avec un critère d'accès, une NAT et une politique de service identiques, l'équilibrage de charges et le routage asymétrique fonctionnent correctement. Nous avons introduit ou modifié les commandes suivantes : **zone**, **zone-member**, **show running-config zone**, **clear configure zone**, **show zone**, **show asp table zone**, **show nameif zone**, **show conn long**, **show local-host zone**, **show route zone**, **show asp table routing**, **clear conn zone**, **clear local-host zone**.
commande **clear local-host**	9.14(1)	La commande **clear local-host** et tous ses attributs et ses mots clés étaient obsolètes. Ils seront supprimés dans une version ultérieure.



PARTIE IV

Paramètres de base

- Paramètres de base, à la page 831
- Services DHCP et DDNS, à la page 857
- Certificats numériques, à la page 885
- Inspection ARP et table des adresses MAC, à la page 925



CHAPITRE 23

Paramètres de base

Ce chapitre décrit comment configurer les paramètres de base sur l'ASA qui sont généralement requis pour une configuration fonctionnelle.

- Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet, à la page 831
- Régler la date et l'heure, à la page 834
- Configurer la phrase secrète principale, à la page 840
- Configurer des serveurs DNS, à la page 844
- Configurer le contournement matériel et l'alimentation double (Cisco ISA 3000), à la page 847
- Modifier les performances et le comportement ASP (Accelerated Security Path), à la page 849
- Supervision du cache DNS, à la page 852
- Historique des paramètres de base, à la page 852

Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet

Pour définir le nom d'hôte, le nom de domaine et les mots de passe d'activation et pour Telnet, procédez comme suit.

Avant de commencer

Avant de définir le nom d'hôte, le nom de domaine et les mots de passe d'activation et pour Telnet, assurez-vous les conditions préalables suivantes sont réunies :

- En mode contexte multiple, vous pouvez configurer le nom d'hôte et le nom de domaine dans les espaces d'exécution du système et du contexte.
- Les mots de passe d'activation et pour Telnet doivent être définis dans chaque contexte. Ils ne sont pas disponibles dans le système.
- Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Précisez le nom d'hôte de l'ASA ou d'un contexte. Le nom d'hôte par défaut est « asa ».

nom d'hôte*nom*

Exemple :

```
ciscoasa(config)# hostname myhostnamexample12345
```

Ce nom peut comporter jusqu'à 63 caractères. Le nom d'hôte doit commencer et se terminer par une lettre ou un chiffre et ne comporter que des lettres, des chiffres ou un tiret.

Lorsque vous définissez un nom d'hôte pour l'ASA, ce nom apparaît dans l'invite de ligne de commande. Si vous établissez des sessions avec plusieurs appareils, le nom d'hôte facilite le suivi de l'emplacement où vous entrez des commandes.

En mode contexte multiple, le nom d'hôte que vous avez défini dans l'espace d'exécution du système apparaît dans l'invite de ligne de commande de tous les contextes. Le nom d'hôte que vous définissez dans un contexte n'apparaît pas sur la ligne de commande, mais il peut être utilisé par le jeton **$(hostname)** de la commande **banner**.

Étape 2 Précisez le nom de domaine de l'ASA. Le nom de domaine par défaut est default.domain.invalid.

domain-name *name*

Exemple :

```
ciscoasa(config)# domain-name example.com
```

L'ASA ajoute le nom de domaine sous forme de suffixe aux noms non qualifiés. Par exemple, si vous définissez le nom de domaine « example.com » et indiquez un serveur syslog sous le nom non qualifié de « jupiter », l'ASA remplace ce nom par « jupiter.example.com ».

Étape 3 Changez le mot de passe d'activation. Par défaut, le mot de passe d'activation est une valeur vide, mais vous êtes invité à la modifier la première fois que vous entrez la commande **enable**.

enable password *password*

Exemple :

```
ciscoasa(config)# enable password Pa$$w0rd
```

Le mot de passe d'activation vous permet de passer en mode d'exécution privilégié si vous ne configurez pas l'authentification d'activation. Le mot de passe d'activation vous permet également de vous connecter à ASDM avec un nom d'utilisateur vide si vous ne configurez pas l'authentification HTTP.

L'argument *password* est un mot de passe sensible à la casse, composé de 8 à 127 caractères. Il peut s'agir de n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), avec les exceptions suivantes :

- Aucun espace
- Aucun point d'interrogation

- Il est interdit d'utiliser trois caractères ASCII (ou plus) qui se suivent ou qui se répètent. Par exemple, les mots de passe suivants seront refusés :
  - **abc**utilisateur1
  - utilisateur**543**
  - utilisateur**aaaa**
  - utilisateur2**666**

Cette commande modifie le mot de passe pour le niveau de privilège le plus élevé (15). Si vous configurez l'autorisation de commande « local », vous pouvez définir des mots de passe d'activation pour chaque niveau de privilège, de 0 à 15, en utilisant la syntaxe suivante :

enable password *password* **level** *number*

Le mot clé **encrypted** (pour les mots de passe de 32 caractères ou moins dans les versions 9.6 et antérieures) ou le mot clé **pbkdf2** (pour les mots de passe de plus de 32 caractères dans les versions 9.6 et ultérieures, et les mots de passe de toutes les longueurs dans les versions 9.7 et ultérieures) indique que le mot de passe est chiffré (à l'aide d'un hachage basé sur MD5 ou d'un hachage PBCDF2 (Password-Based Key Derivation Function 2) utilisant SHA-512). Notez que les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Lorsque vous définissez un mot de passe dans la commande **enable password**, l'ASA le chiffre avant de l'enregistrer dans la configuration à des fins de sécurité. Lorsque vous entrez la commande **show running-config**, la commande **enable password** n'affiche pas le mot de passe réel. Elle affiche le mot de passe chiffré suivi du mot clé **encrypted** ou **pbkdf2**. Par exemple, si vous entrez le mot de passe « test », la sortie de la commande **show running-config** se présentera comme suit :

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

Vous ne saisirez le mot clé **encrypted** ou **pbkdf2** dans l'interface de ligne de commande que si vous coupez-collez un fichier de configuration pour l'utiliser dans un autre ASA et que vous utilisez le même mot de passe.

Vous ne pouvez pas réinitialiser le mot de passe à une valeur vide.

Étape 4 Définissez le mot de passe de connexion pour l'accès Telnet. Il n'y a pas de mot de passe par défaut.

Le mot de passe de connexion est utilisé pour l'accès Telnet si vous ne configurez pas l'authentification Telnet.

passwd *password* [**encrypted**]

Exemple :

```
ciscoasa(config)# passwd cisco12345
```

Le *mot de passe* est sensible à la casse et peut comporter jusqu'à 16 caractères alphanumériques et spéciaux. Vous pouvez utiliser n'importe quel caractère dans le mot de passe, à l'exception d'un point d'interrogation ou d'un espace.

Le mot de passe est enregistré dans la configuration sous une forme chiffrée, ce qui vous empêche de voir le mot de passe d'origine après l'avoir saisi. Si, pour une raison quelconque, vous devez copier le mot de passe dans un autre ASA, mais que vous ne connaissez pas le mot de passe d'origine, vous pouvez saisir la commande

passwd avec le mot de passe chiffré et le mot clé **encrypted**. Normalement, vous ne voyez ce mot clé que lorsque vous entrez la commande **show running-config passwd**.

Régler la date et l'heure

Remarque Ne définissez pas la date et l'heure de de Firepower 2100 en mode plateforme, 4100/9300; l'ASA reçoit ces paramètres du châssis.

Définir les dates des fuseaux horaires et de l'heure avancée

Pour définir le fuseau horaire et la plage de dates de l'heure avancée, procédez comme suit.

Procédure

Étape 1 Définissez le fuseau horaire. Par défaut, le fuseau horaire est UTC.

- Modèles Firepower et Secure Firewall :

  clock timezone *zone*

  - *zone* : saisissez la commande **clock timezone ?** pour afficher une liste de noms de fuseau horaire acceptables.

  Exemple :

```
ciscoasa(config)# clock timezone ?
Available timezones:
CET
CST6CDT
Cuba
EET
Egypt
Eire
EST
EST5EDT
Factory
GB
GB-Eire
GMT
GMT0
GMT-0
GMT+0
Greenwich
Hongkong
HST
Iceland
Iran
Israel
Jamaica
```

```
Japan
[...]

ciscoasa(config)# clock timezone US/?

configure mode commands/options:
  US/Alaska          US/Aleutian    US/Arizona    US/Central
  US/East-Indiana    US/Eastern     US/Hawaii     US/Indiana-Starke
  US/Michigan        US/Mountain    US/Pacific

ciscoasa(config)# clock timezone US/Mountain
```

- Tous les autres modèles :

  clock timezone *zone* [-]*hours* [*minutes*]

  - *zone* : spécifie le fuseau horaire en tant que chaîne, par exemple, PST pour l'heure standard du Pacifique.
  - [-]*hours* : définit le nombre d'heures de décalage par rapport à l'heure UTC. Par exemple, PST est de -8 heures.
  - *minutes* : définit le nombre de minutes de décalage par rapport à l'heure UTC.

  Exemple :

```
ciscoasa(config)# clock timezone PST -8
```

Étape 2 (ASA virtuel et ISA 3000) Saisissez l'une des commandes suivantes pour modifier la plage de dates pour l'heure avancée à partir de la valeur par défaut. La plage de dates récurrentes par défaut va de 2 h le deuxième dimanche de mars à 2 h le premier dimanche de novembre.

- Définissez les dates de début et de fin de l'heure avancée comme date précise dans une année donnée. Si vous utilisez cette commande, vous devez réinitialiser les dates chaque année.

  clock summer-time *zone* **date** {*day month* | *month day*} *year hh***:***mm* {*day month* | *month day*} *year hh***:***mm* [*offset*]

  - *zone* : spécifie le fuseau horaire sous forme de chaîne, par exemple, PDT pour l'heure avancée du centre.
  - *day* : définit le jour du mois, de 1 à 31. Vous pouvez saisir le jour et le mois comme **a**vril 1er ou 1er avril, par exemple, selon votre format de date standard.
  - *month* : définit le mois sous la forme d'une chaîne de caractères. Vous pouvez saisir le jour et le mois comme avril 1er ou 1er avril, selon votre format de date standard.
  - *year* : définit l'année en utilisant quatre chiffres, par exemple, 2004. La plage d'années va de 1993 à 2035.
  - *hh:mm* : définit l'heure et les minutes sur 24 heures.
  - *offset* : définit le nombre de minutes pour modifier l'heure pour l'heure avancée. Par défaut, la valeur est de 60 minutes.

  Exemple :

```
ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60
```

- Spécifiez les dates de début et de fin de l'heure avancée, sous la forme d'un jour et d'une heure du mois, et non d'une date précise dans une année. Cette commande vous permet de définir une plage de dates récurrentes que vous n'avez pas besoin de modifier chaque année.

  clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

  - *zone* : spécifie le fuseau horaire sous forme de chaîne, par exemple, PDT pour l'heure avancée du centre.
  - *week* : spécifie la semaine du mois sous la forme d'un nombre entier compris entre 1 et 4 ou avec les mots « première » ou « dernière ». Par exemple, si le jour peut tomber sur la cinquième semaine, précisez « dernière ».
  - *weekday* : spécifie le jour de la semaine : lundi, mardi, mercredi, etc.
  - *month* : définit le mois sous la forme d'une chaîne de caractères.
  - *hh:mm* : définit l'heure et les minutes sur 24 heures.
  - *offset* : définit le nombre de minutes pour modifier l'heure pour l'heure avancée. Par défaut, la valeur est de 60 minutes.

  Exemple :

```
ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60
```

Définir la date et l'heure à l'aide du serveur NTP

Le protocole NTP est utilisé pour mettre en œuvre un système hiérarchique de serveurs qui fournissent une heure synchronisée avec précision entre les systèmes du réseau. Ce type de précision est requis pour les opérations urgentes, telles que la validation de listes de révocation de certificats, qui comprennent un horodatage précis. Vous pouvez configurer plusieurs serveurs NTP. L'ASA choisit le serveur avec la strate la plus basse, qui est une mesure de la fiabilité des données.

L'heure dérivée d'un serveur NTP remplace toute heure définie manuellement.

L'ASA prend en charge NTPv4.

Avant de commencer

En mode de contexte multiple, vous pouvez définir l'heure dans la configuration système uniquement.

Procédure

Étape 1 (Facultatif) Activez l'authentification avec un serveur NTP.

a) Activez l'authentification.

ntp authenticate

Exemple :

```
ciscoasa(config)# ntp authenticate
```

Lorsque vous activez l'authentification NTP, vous devez également spécifier un ID de clé dans la commande **ntp trusted-key** et associer cette clé au serveur à l'aide de la commande **ntp server key**. Configurez la clé réelle pour l'ID à l'aide de la commande **ntp authentication-key**. Si vous avez plusieurs serveurs, configurez un ID distinct pour chaque serveur.

b) Spécifiez un ID de clé d'authentification comme clé de confiance, qui est nécessaire pour l'authentification auprès d'un serveur NTP.

ntp trusted-key *key_id*

Exemple :

```
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
```

L'argument *key_id* est une valeur comprise entre 1 et 4294967295. Vous pouvez saisir plusieurs clés de confiance à utiliser avec plusieurs serveurs.

c) Définissez une clé pour vous authentifier auprès d'un serveur NTP.

ntp authentication-key *key_id* {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} *key*

Exemple :

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey1
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
```

- *key_id* : définit l'ID que vous avez défini à l'aide de la commande **ntp trusted-key**.
- {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} : définit l'algorithme.
- *key* : définit la clé sous la forme d'une chaîne pouvant comporter jusqu'à 32 caractères.

Étape 2 Identifiez un serveur NTP.

ntp server {*ipv4_address* | *ipv6_address* }[**key** *key_id*] [**source** *interface_name*] [**prefer**]

Exemple :

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp server 2001:DB8::178 key 3
ciscoasa(config)# ntp server 2001:DB8::8945:ABCD key 4
```

Si vous avez activé l'authentification NTP (**ntp authenticate**), vous devez spécifier l'argument **key** *key_id* à l'aide de l'ID que vous avez défini à l'aide de la commande **ntp trusted-key**.

La paire mot clé-argument **source** *interface_name* identifie l'interface sortante pour les paquets NTP si vous ne souhaitez pas utiliser l'interface par défaut dans la table de routage. Étant donné que le système n'inclut aucune interface en mode de contexte multiple, spécifiez un nom d'interface défini dans le contexte d'administration.

Le mot clé **prefer** définit ce serveur NTP comme le serveur préféré si plusieurs serveurs ont une précision similaire. Le NTP utilise un algorithme pour déterminer quel serveur est le plus précis et se synchronise avec celui-ci. Si les serveurs sont de précision similaire, le mot clé **prefer** spécifie lequel de ces serveurs utiliser. Cependant, si un serveur est nettement plus précis que le serveur préféré, l'ASA utilise le plus précis. Par exemple, l'ASA utilise un serveur de strate 2 plutôt qu'un serveur de strate 3 qui est préféré.

Vous pouvez identifier plusieurs serveurs; l'ASA utilise le serveur le plus précis.

Régler la date et l'heure manuellement

Pour définir la date et l'heure manuellement, procédez comme suit :

Avant de commencer

En mode de contexte multiple, vous pouvez définir l'heure dans la configuration système uniquement.

Procédure

Réglez la date et l'heure manuellement.

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

Exemple :

```
ciscoasa# clock set 20:54:00 april 1 2004
```

L'argument *hh*:*mm*:*ss* définit l'heure, les minutes et les secondes sur 24 heures. Par exemple, saisissez 20:54:00 pour 20:54.

La valeur du jour définit le jour du mois, de 1 à 31. Vous pouvez saisir le jour et le mois comme avril 1er ou 1er avril, par exemple, selon votre format de date standard.

La valeur du mois définit le mois. Selon votre format de date standard, vous pouvez saisir le jour et le mois comme avril 1er ou 1er avril.

La valeur de l'année définit l'année en utilisant quatre chiffres, par exemple, 2004. La fourchette d'années va de 1993 à 2035.

Le fuseau horaire par défaut est UTC. Si vous modifiez le fuseau horaire après avoir saisi la commande **clock set** à l'aide de la commande **clock timezone**, l'heure s'ajuste automatiquement au nouveau fuseau horaire.

Cette commande règle l'heure dans la puce matérielle et n'enregistre pas l'heure dans le fichier de configuration. Cette heure résiste aux redémarrages. Contrairement aux autres commandes **clock**, celle-ci est une commande

EXEC privilégée. Pour réinitialiser l'horloge, vous devez régler une nouvelle heure avec la commande clock set.

Configurer le protocole PTP (Precision Time Protocol) (ISA 3000)

Le protocole PTP (Precision Time Protocol) est un protocole de synchronisation horaire développé pour synchroniser les horloges de divers périphériques au sein d'un réseau par paquets. Ces horloges sont généralement de précision et de stabilité variables. Le protocole est spécialement conçu pour les systèmes de mesure et de contrôle industriels en réseau. Il est idéal pour une utilisation dans les systèmes distribués, car il nécessite une bande passante et un surdébit de traitement minimaux.

Un système PTP est un système en réseau distribué, composé d'une combinaison de périphériques PTP et non-PTP. Les périphériques PTP comprennent les horloges normales, les horloges périphériques et les horloges transparentes. Les périphériques non PTP comprennent les commutateurs réseau, les routeurs et les autres périphériques de l'infrastructure.

Vous pouvez configurer l'ASA pour qu'il soit une horloge transparente. L'ASA ne synchronise pas son horloge avec les horloges PTP. L'ASA utilisera le profil PTP par défaut, comme défini sur les horloges PTP.

Lorsque vous configurez les périphériques PTP, vous définissez un numéro de domaine pour les périphériques qui sont destinés à fonctionner ensemble. Ainsi, vous pouvez configurer plusieurs domaines PTP, puis configurer chaque périphérique non PTP pour qu'il utilise les horloges PTP d'un domaine spécifique.

Avant de commencer

- Cette fonctionnalité est uniquement disponible sur l'ISA 3000.
- L'utilisation du PTP n'est prise en charge qu'en mode de contexte unique.
- Cisco PTP prend uniquement en charge les messages PTP en multidiffusion.
- Le PTP est activé sur toutes les interfaces ISA 3000 en mode transparent par défaut. En mode routé, vous devez ajouter la configuration nécessaire pour vous assurer que les paquets PTP sont autorisés à transiter par le périphérique.
- Le PTP est disponible uniquement pour les réseaux IPv4, et non pour les réseaux IPv6.
- La configuration PTP est prise en charge sur les interfaces Ethernet physiques, qu'elles soient autonomes ou membres d'un groupe de ponts. Elle n'est pas prise en charge sur :
    - Interface de gestion.
    - Sous-interfaces, EtherChannels, BVI ou toute autre interface virtuelle.
- Les flux PTP sur les sous-interfaces VLAN sont pris en charge, en supposant que la configuration PTP appropriée est présente sur l'interface parente.
- Vous devez vous assurer que les paquets PTP sont autorisés à circuler dans le périphérique. En mode de pare-feu transparent, la configuration de la liste d'accès permettant le trafic PTP est configurée par défaut. Le trafic PTP est identifié par les ports UDP 319 et 320 et par l'adresse IP de destination 224.0.1.129. Ainsi, en mode de pare-feu routé, toute liste ACL autorisant ce trafic devrait être acceptable.
- En mode de pare-feu routé, vous devez également activer le routage de multidiffusion pour les groupes de multidiffusion PTP :

- Entrez la commande du mode de configuration globale **multicast-routing**.
- Et pour chaque interface qui n'est pas membre d'un groupe de ponts et sur laquelle le protocole PTP est activé, saisissez la commande de configuration d'interface **igmp join-group 224.0.1.129** pour activer statiquement l'appartenance au groupe de multidiffusion PTP. Cette commande n'est pas prise en charge ni nécessaire pour les membres du groupe de ponts.

Procédure

Étape 1 Spécifiez le numéro de domaine de tous les ports du périphérique :

ptp domain *domain_num*

Exemple :

```
ciscoasa(config)# ptp domain 54
```

L'argument *domain_num* est le numéro de domaine de tous les ports du périphérique. Les paquets reçus dans un domaine différent sont traités comme des paquets de multidiffusion ordinaires et ne subissent aucun traitement PTP. Cette valeur peut aller de zéro à 255; la valeur par défaut est zéro. Saisissez le numéro de domaine configuré sur les périphériques PTP de votre réseau.

Étape 2 (Facultatif) Configurez le mode d'horloge PTP sur le périphérique :

ptp mode e2etransparent

Exemple :

```
ciscoasa(config)# ptp mode e2etransparent
```

Cette commande active le mode transparent de bout en bout sur toutes les interfaces compatibles avec PTP.

Étape 3 Activez PTP sur une interface :

ptp enable

Activez PTP sur chaque interface par laquelle le système peut communiquer avec une horloge PTP dans le domaine configuré.

Exemple :

```
ciscoasa(config)# interface gigabitethernet1/2
ciscoasa(config-if)# ptp enable
```

Configurer la phrase secrète principale

La phrase secrète principale vous permet de stocker en toute sécurité les mots de passe en texte brut dans un format chiffré et fournit une clé utilisée pour chiffrer ou masquer tous les mots de passe de manière universelle, sans modifier aucune fonctionnalité. Voici les fonctionnalités qui utilisent la phrase secrète principale :

- OSPF
- EIGRP

- Équilibrage de la charge VPN
- VPN (accès à distance et de site à site)
- Basculement
- Serveurs AAA
- Logging (journalisation)
- Licences partagées

Ajouter ou modifier la phrase secrète principale

Pour ajouter ou modifier la phrase secrète principale, procédez comme suit.

Avant de commencer

- Cette procédure ne sera acceptée que dans une session sécurisée, par exemple par la console, SSH ou ASDM via HTTPS.
- Si le basculement est activé, mais qu'aucune clé partagée de basculement n'est définie, un message d'erreur s'affiche si vous modifiez la phrase secrète principale, vous informant que vous devez saisir une clé partagée de basculement pour protéger les modifications de phrase secrète principale contre l'envoi en texte brut.
- L'activation ou la modification du chiffrement par mot de passe dans le basculement actif/veille entraîne un **write standby**, qui réplique la configuration active sur l'unité de secours. Sans cette réplication, les mots de passe chiffrés sur l'unité de secours seront différents, même s'ils utilisent la même phrase secrète; la réplication de la configuration garantit que les configurations sont identiques. Pour le basculement actif/actif, vous devez saisir manuellement **write standby**. Un **write standby** peut entraîner une interruption du trafic en mode actif/actif, car la configuration est effacée sur l'unité secondaire avant que la nouvelle configuration ne soit synchronisée. Vous devez activer tous les contextes sur l'ASA principal à l'aide des commandes **failover active group 1** et **failover active group 2**, saisir **write standby**, puis restaurer les contextes du groupe 2 sur l'unité secondaire à l'aide de la commande **no failover active group 2**.

Procédure

Étape 1 Définissez la phrase secrète utilisée pour générer la clé de chiffrement. La phrase secrète doit comporter de 8 à 128 caractères. Tous les caractères, à l'exception de la touche retour arrière et des guillemets doubles, sont acceptés pour la phrase secrète. Si vous ne saisissez pas la nouvelle phrase secrète dans la commande, vous serez invité à la saisir. Pour modifier la phrase secrète, vous devez saisir l'ancienne phrase secrète.

key config-key password-encryption [*new_passphrase* [*old_passphrase*]]

Exemple :

```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

Remarque
Utilisez les invites interactives pour saisir les mots de passe afin d'éviter que les mots de passe soient enregistrés dans le tampon de l'historique des commandes.

Utilisez la commande **no key config-key password-encrypt** avec prudence, car elle change les mots de passe chiffrés en mots de passe en texte brut. Vous pouvez utiliser la forme **no** de cette commande lors de la rétrogradation à une version logicielle qui ne prend pas en charge le chiffrement des mots de passe.

Étape 2 Activez le chiffrement des mots de passe.

password encryption aes

Exemple :

```
ciscoasa(config)# password encryption aes
```

Dès que le chiffrement des mots de passe est activé et que la phrase secrète principale est disponible, tous les mots de passe des utilisateurs seront chiffrés. La configuration en cours d'exécution affichera les mots de passe dans le format chiffré.

Si la phrase secrète n'est pas configurée au moment où le chiffrement du mot de passe est activé, la commande réussira en prévision de la disponibilité future de la phrase secrète.

Si vous désactivez ultérieurement le chiffrement des mots de passe à l'aide de la commande **no password encryption aes**, tous les mots de passe chiffrés existants resteront inchangés et, tant que la phrase secrète principale existe, les mots de passe chiffrés seront déchiffrés, comme l'exige l'application.

Étape 3 Enregistrez la valeur d'exécution de la phrase secrète principale et la configuration résultante.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Si vous ne saisissez pas cette commande, les mots de passe de la configuration de démarrage peuvent toujours être visibles s'ils n'ont pas été enregistrés pour le chiffrement précédemment. De plus, en mode de contexte multiple, le mot de passe principal est modifié dans la configuration du contexte système. Par conséquent, les mots de passe de tous les contextes seront affectés. Si la commande write memory n'est pas saisie en mode de contexte système, mais pas dans tous les contextes d'utilisateur, les mots de passe chiffrés dans les contextes d'utilisateur peuvent être obsolètes. Vous pouvez également utiliser la commande write memory all dans le contexte système pour enregistrer toutes les configurations.

Exemples

L'exemple suivant montre qu'aucune clé n'existait auparavant :

```
ciscoasa(config)# key config-key password-encryption 12345678
```

L'exemple suivant montre qu'une clé existe déjà :

```
ciscoasa(config)# key config-key password-encryption 23456789
Old key: 12345678
```

Dans l'exemple suivant, vous saisissez la commande sans paramètres afin que le système vous demande les clés. Comme une clé existe déjà, vous êtes invité à l'utiliser.

```
ciscoasa(config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

Dans l'exemple suivant, il n'y a pas de clé existante, vous n'êtes donc pas invité à la fournir.

```
ciscoasa(config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

Désactiver la phrase secrète principale

La désactivation de la phrase secrète principale rétablit les mots de passe chiffrés en mots de passe en texte brut. Supprimer la phrase secrète peut être utile si vous rétrogradez à une version précédente du logiciel qui ne prend pas en charge les mots de passe chiffrés.

Avant de commencer

- Vous devez connaître la phrase secrète principale actuelle pour la désactiver. Consultez Supprimer la phrase secrète principale, à la page 844 si vous ne connaissez pas la phrase secrète.
- Cette procédure fonctionne uniquement dans une session sécurisée; c'est-à-dire par Telnet, SSH ou ASDM via HTTPS.

  Pour désactiver la phrase secrète principale, procédez comme suit :

Procédure

Étape 1 Supprimez la phrase secrète principale. Si vous ne saisissez pas la phrase secrète dans la commande, vous serez invité à la saisir.

no key config-key password-encryption [*old_passphrase*]]

Exemple :

```
ciscoasa(config)# no key config-key password-encryption

Warning! You have chosen to revert the encrypted passwords to plain text.
This operation will expose passwords in the configuration and therefore
exercise caution while viewing, storing, and copying configuration.

Old key: bumblebee
```

Étape 2 Enregistrez la valeur d'exécution de la phrase secrète principale et la configuration résultante.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

La mémoire non volatile contenant la phrase secrète sera effacée et remplacée par le modèle 0xFF.

En mode multiple, la phrase secrète principale est modifiée dans la configuration du contexte système. Par conséquent, les mots de passe de tous les contextes seront affectés. Si la commande write memory est saisie en mode de contexte système, mais pas dans tous les contextes d'utilisateur, les mots de passe chiffrés dans les contextes d'utilisateur peuvent être obsolètes. Vous pouvez également utiliser la commande write memory all dans le contexte système pour enregistrer toutes les configurations.

Supprimer la phrase secrète principale

Vous ne pouvez pas récupérer la phrase secrète principale. Si la phrase secrète principale est perdue ou inconnue, vous pouvez la supprimer.

Pour supprimer la phrase secrète principale, procédez comme suit :

Procédure

Étape 1 Supprimez la clé principale et la configuration qui comprend les mots de passe chiffrés.

write erase

Exemple :

```
ciscoasa(config)# write erase
```

Étape 2 Rechargez l'ASA avec la configuration de démarrage, sans clé principale ni mot de passe chiffré.

reload

Exemple :

```
ciscoasa(config)# reload
```

Configurer des serveurs DNS

Vous devez configurer un serveur DNS pour que l'ASA puisse résoudre les noms d'hôte en adresses IP. Vous devez également configurer un serveur DNS pour utiliser des objets réseau de noms de domaine complets (FQDN) dans les critères d'accès.

Certaines fonctionnalités de l'ASA nécessitent l'utilisation d'un serveur DNS pour accéder aux serveurs externes par nom de domaine. D'autres fonctionnalités, telles que la commande **ping** ou **traceroute**, vous permettent de saisir un nom que vous souhaitez envoyer par message Ping ou par route de trace. L'ASA peut résoudre le nom en communiquant avec un serveur DNS. De nombreuses commandes SSL VPN et de certificat prennent également en charge les noms.

Par défaut, il existe un groupe de serveurs DNS par défaut appelé DefaultDNS. Vous pouvez créer plusieurs groupes de serveurs DNS : un groupe est le groupe par défaut, tandis que les autres groupes peuvent être associés à des domaines spécifiques. Une requête DNS qui correspond à un domaine associé à un groupe de serveurs DNS utilisera ce groupe. Par exemple, si vous souhaitez que le trafic destiné aux serveurs internes eng.cisco.com utilise un serveur DNS interne, vous pouvez mapper eng.cisco.com à un groupe DNS interne. Toutes les requêtes DNS qui ne correspondent pas à un mappage de domaine utiliseront le groupe de serveurs DNS par défaut, qui n'a pas de domaine associé. Par exemple, le groupe DefaultDNS peut inclure un serveur DNS public disponible sur l'interface externe. D'autres groupes de serveurs DNS peuvent être configurés pour les groupes de tunnels VPN. Consultez la commande **tunnel-group** dans la référence de commande pour en savoir plus.



Remarque L'ASA a une prise en charge limitée pour l'utilisation du serveur DNS, en fonction de la fonctionnalité. Par exemple, la plupart des commandes nécessitent que vous saisissiez une adresse IP et ne peuvent utiliser un nom que lorsque vous configurez manuellement la commande **name** pour associer un nom à une adresse IP et permettre l'utilisation des noms à l'aide de la commande names.

Avant de commencer

Assurez-vous de configurer les règles de routage et d'accès appropriées pour toute interface sur laquelle vous activez la recherche de domaine DNS afin de pouvoir atteindre le serveur DNS.

Procédure

Étape 1 Permettez à l'ASA d'envoyer des requêtes DNS à un serveur DNS afin d'effectuer une recherche de nom pour les commandes prises en charge.

dns domain-lookup *interface_name*

Si vous n'activez pas la recherche DNS sur une interface, l'ASA ne communiquera pas avec le serveur DNS sur cette interface. Assurez-vous d'activer la recherche DNS sur toutes les interfaces qui seront utilisées pour accéder aux serveurs DNS.

Exemple :

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns domain-lookup outside
```

Étape 2 Créez un ou plusieurs groupes de serveurs DNS et ajoutez des serveurs aux groupes.

a) Nommez le groupe de serveurs DNS.

dns server-group *name*

Pour configurer le groupe de serveurs DefaultDNS par défaut, spécifiez DefaultDNS comme nom.

Exemple :

```
ciscoasa(config)# dns server-group DefaultDNS
```

b) Spécifiez un ou plusieurs serveurs DNS pour le groupe.

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*] *[interface_name]*

Vous pouvez saisir les six adresses IP dans la même commande, séparées par des espaces, ou vous pouvez saisir chaque commande séparément.

(Facultatif) Spécifiez le *nom de l'interface* par lequel l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage des données; s'il n'y a aucune correspondance, il vérifie la table de routage de gestion uniquement.

L'ASA essaie chaque serveur DNS dans l'ordre jusqu'à ce qu'il reçoive une réponse.

Exemple :

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6 outside
```

c) (Pour le groupe par défaut uniquement) Configurez le nom de domaine ajouté au nom d'hôte s'il n'est pas entièrement qualifié.

domain-name *name*

Exemple :

```
ciscoasa(config-dns-server-group)# domain-name example.com
```

d) (Facultatif) Configurez les propriétés supplémentaires du groupe de serveurs DNS.

Utilisez les commandes suivantes pour modifier les caractéristiques du groupe, si les paramètres par défaut ne conviennent pas à votre réseau.

- **timeout** *seconds* : le nombre de secondes, de 1 à 30, à attendre avant d'essayer le serveur DNS suivant. La valeur par défaut est de 2 secondes. Chaque fois que l'ASA réessaie la liste des serveurs, ce délai est doublé.
- **retries** *number* : le nombre de tentatives, de 0 à 10, pour retenter d'accéder à la liste des serveurs DNS lorsque l'ASA ne reçoit pas de réponse.
- **expire-entry-timer minutes** *number* : la TTL minimum pour l'entrée DNS, en minutes. Si le délai d'expiration est plus long que la durée de vie de l'entrée, cette dernière est augmentée jusqu'à la valeur du délai d'expiration de l'entrée. Si la durée de vie est plus longue que le délai d'expiration, la valeur du délai d'expiration est ignorée : dans ce cas, aucun délai supplémentaire n'est ajouté à la durée de vie. À l'expiration, l'entrée est supprimée de la table de consultation du DNS. La suppression d'une entrée nécessite la recompilation de la table, de sorte que des suppressions fréquentes peuvent augmenter la charge de traitement du périphérique. Comme certaines entrées DNS peuvent avoir une durée de vie très courte (jusqu'à trois secondes), vous pouvez utiliser ce paramètre pour prolonger virtuellement cette dernière. La valeur par défaut est 1 minute (c'est-à-dire que la durée de vie minimale pour toutes les résolutions est de 1 minute). La plage est comprise entre 1 et 65535 minutes. Cette option est utilisée uniquement pour la résolution d'objets réseau FQDN.

- **poll-timer minutes** *number* : la durée, en minutes, du cycle d'interrogation utilisé pour résoudre les objets réseau/hôte FQDN en adresses IP. Les objets FQDN ne sont résolus que s'ils sont utilisés dans une politique de pare-feu. La minuterie détermine le temps maximum entre les résolutions; la valeur de durée de vie (TTL) de l'entrée DNS est également utilisée pour déterminer quand mettre à jour la résolution d'adresse IP, de sorte que les FQDN individuels puissent être résolus plus fréquemment que le cycle d'interrogation. La valeur par défaut est 240 (quatre heures). La plage est comprise entre 1 et 65535 minutes.

e) Répétez les étapes ci-dessus pour ajouter des groupes de serveurs DNS supplémentaires.

Étape 3 (Facultatif) Mappez les domaines à des groupes de serveurs DNS spécifiques.

dns-group-map

dns-to-domain *dns_group_name domain*

Vous pouvez mapper jusqu'à 30 domaines. Vous ne pouvez pas mapper le même domaine à plusieurs groupes de serveurs DNS, mais vous pouvez mapper plusieurs domaines au même groupe de serveurs. Ne mappez aucun domaine au groupe que vous souhaitez utiliser par défaut (par exemple, DefaultDNS).

Exemple :

```
ciscoasa(config)# dns-group-map
ciscoasa(config-dns-group-map)# dns-to-domain group1 eng.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group1 hr.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group2 example.com
```

Étape 4 Spécifiez le groupe DNS par défaut.

dns-group *name*

Par défaut, DefaultDNS est spécifié. Si vous avez configuré d'autres groupes, vous pouvez définir un groupe par défaut différent à l'aide de cette commande. Le groupe par défaut ne peut avoir aucun domaine associé dans la carte des groupes DNS.

Exemple :

```
ciscoasa(config)# dns-group new_default_group
```

Configurer le contournement matériel et l'alimentation double (Cisco ISA 3000)

Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Les paires d'interfaces prises en charge sont les interfaces en cuivre GigabitEthernet 1/1 et 1/2; et GigabitEthernet 1/3 et 1/4. Lorsque le contournement matériel est actif, aucune fonction de pare-feu n'est en place. Veuillez donc vous assurer de bien comprendre les risques liés à l'autorisation du trafic de transit. Consultez les lignes directrices suivantes relatives au contournement matériel :

- Cette fonctionnalité est uniquement disponible sur le périphérique Cisco ISA 3000.
- Si vous avez un modèle Ethernet à fibre optique, seule la paire Ethernet en cuivre (GigabitEthernet 1/1 et 1/2) prend en charge le contournement matériel.

- Lorsque l'ISA 3000 perd de l'alimentation et passe en mode de contournement matériel, seules les paires d'interfaces prises en charge peuvent communiquer; avec la configuration par défaut, inside1 <---> inside2 et outside1 <---> outside2 ne peuvent plus communiquer. Toutes les connexions existantes entre ces interfaces seront perdues.
- Nous vous suggérons de désactiver la répartition aléatoire des séquences TCP (comme le décrit cette procédure). Si la répartition aléatoire est activée (par défaut), lorsque le contournement matériel sera activé, les sessions TCP devront être rétablies. Par défaut, l'ISA 3000 réécrit le numéro de séquence initial (ISN) des connexions TCP qui le traversent en nombre aléatoire. Lorsque le contournement matériel est activé, l'ISA 3000 ne se trouve plus dans le chemin de données et ne traduit pas les numéros de séquence; le client destinataire reçoit un numéro de séquence inattendu et interrompt la connexion. Même lorsque la répartition aléatoire de la séquence TCP est désactivée, certaines connexions TCP devront être rétablies car la liaison a été temporairement interrompue pendant le basculement.
- Les connexions Cisco TrustSec sur les interfaces de contournement matériel sont abandonnées lorsque le contournement matériel est activé. Lorsque l'ISA 3000 démarre et que le contournement matériel est désactivé, les connexions sont renégociées.
- Lorsque le contournement matériel est désactivé et que le trafic reprend par le chemin de données de l'ISA 3000, certaines sessions TCP existantes doivent être rétablies en raison de la liaison qui est temporairement inactive pendant le basculement.
- Lorsque le contournement matériel est actif, les PHY Ethernet sont déconnectés, de sorte que l'ASA ne peut pas déterminer l'état de l'interface. Les interfaces peuvent sembler être en panne.

Pour les alimentations doubles dans l'ISA 3000, vous pouvez établir des alimentations doubles comme la configuration attendue dans le système d'exploitation ASA. En cas de défaillance d'une alimentation, l'ASA émet une alarme. Par défaut, l'ASA s'attend à une seule alimentation et n'émettra pas d'alarme tant qu'il dispose d'une alimentation opérationnelle.

Avant de commencer

- Vous devez connecter les interfaces de contournement matériel pour accéder aux ports du commutateur. Ne les connectez pas aux ports de ligne principale.

Procédure

Étape 1 Configurez le contournement matériel pour qu'il s'active en cas de panne de courant :

hardware-bypass GigabitEthernet {**1/1-1/2** | **1/3-1/4**} [**sticky**]

Exemple :

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

Le mot clé **sticky** maintient l'appareil en mode de contournement matériel après le rétablissement du courant et le démarrage de l'appareil. Dans ce cas, vous devez désactiver manuellement le contournement matériel lorsque vous êtes prêt; cette option vous permet de contrôler le moment où une brève interruption du trafic se produit.

Étape 2 Activez ou désactivez manuellement le contournement matériel :

[**no**] **hardware-bypass manual GigabitEthernet** {**1/1-1/2** | **1/3-1/4**}

Exemple :

```
ciscoasa# hardware-bypass manual GigabitEthernet 1/1-1/2
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

Étape 3 (Facultatif) Configurez le contournement matériel pour qu'il reste actif jusqu'après le démarrage du module ASA FirePOWER :

hardware-bypass boot-delay module-up sfr

Vous devez activer le contournement matériel sans l'option **sticky** (rémanence) pour que le délai de démarrage fonctionne. Sans la commande **hardware-bypass boot-delay**, le contournement matériel risque de devenir inactif avant la fin du démarrage du module ASA FirePOWER. Ce scénario peut entraîner l'abandon du trafic si vous avez configuré le module en cas de non-conformité, par exemple.

Étape 4 Désactivez la gestion aléatoire de la séquence TCP. Cet exemple montre comment désactiver la répartition aléatoire pour tout le trafic en ajoutant le paramètre à la configuration par défaut.

policy-map global_policy

class sfrclass

set connection random-sequence-number disable

Si vous décidez de le réactiver ultérieurement, remplacez « disable » par **enable**.

Étape 5 Établissez les alimentations doubles comme configuration attendue :

power-supply dual

Étape 6 Enregistrez la configuration.

write memory

Le comportement du contournement matériel après la mise en ligne du système est déterminé par les paramètres de configuration dans la configuration de démarrage. Vous devez donc enregistrer votre configuration en cours d'exécution.

Modifier les performances et le comportement ASP (Accelerated Security Path)

L'ASP est une couche d'implémentation qui met en œuvre vos politiques et vos configurations. Elle ne présente pas d'intérêt direct, sauf lors de la résolution de problèmes avec le centre d'assistance technique Cisco. Cependant, il existe certains comportements liés aux performances et à la fiabilité que vous pouvez ajuster.

Choisir un modèle de validation transactionnelle de moteur de règles

Par défaut, lorsque vous modifiez une politique basée sur des règles (comme des critères d'accès), les modifications prennent effet immédiatement. Cependant, cette immédiateté s'accompagne d'une légère perte de performances. Cette perte de performances est plus notable pour les très grandes listes de règles dans un

environnement à haut débit de connexions par seconde, par exemple lorsque vous modifiez une stratégie comportant 25 000 règles alors que l'ASA traite 18 000 connexions par seconde.

Les performances sont affectées, car le moteur de règles compile des règles pour accélérer la recherche de règles. Par défaut, le système recherche également les règles non compilées lors de l'évaluation d'une tentative de connexion afin que de nouvelles règles puissent être appliquée; comme les règles ne sont pas compilées, la recherche prend plus de temps.

Vous pouvez modifier ce comportement pour que le moteur de règles utilise un modèle transactionnel lors de la mise en œuvre des modifications de règles, en continuant à utiliser les anciennes règles jusqu'à ce que les nouvelles règles soient compilées et prêtes à l'emploi. Avec le modèle transactionnel, les performances ne devraient pas baisser pendant la compilation des règles. Le tableau suivant clarifie la différence de comportement.

Modèle	Avant la compilation	Pendant la compilation	Après la compilation
Par défaut	Correspond aux anciennes règles.	Correspondance avec les nouvelles règles. (Le débit de connexions par seconde diminue.)	Correspond aux nouvelles règles.
Transactionnel	Correspond aux anciennes règles.	Correspondance avec les anciennes règles. (Le débit de connexions par seconde n'est pas affecté.)	Correspond aux nouvelles règles.

Un avantage supplémentaire du modèle transactionnel est que, lors du remplacement d'une ACL sur une interface, il n'y a aucun intervalle entre la suppression de l'ancienne ACL et l'application de la nouvelle. Cette fonctionnalité réduit le risque que des connexions acceptables soient abandonnées pendant l'opération.

Avant de commencer

- La validation transactionnelle n'est pas conseillée pour les règles de contrôle d'accès si vous utilisez des objets FQDN pour des noms d'hôte dont la résolution peut changer fréquemment, car la compilation du groupe d'accès pourrait ne jamais aboutir complètement en raison des fluctuations DNS. Si vous souhaitez tout de même utiliser la validation transactionnelle, envisagez d'allonger le délai d'expiration du DNS.
- Si vous activez le modèle transactionnel pour un type de règle, des journaux système marquant le début et la fin de la compilation sont générés. Ces journaux système sont numérotés de 780 001 à 780 004.

Procédure

Activez le modèle de validation transactionnelle pour le moteur de règles :

asp rule-engine transactional-commit *option*

Où les options sont les suivantes :

- **access-group** : critères d'accès appliqués globalement ou aux interfaces.
- **nat** : règles de traduction des adresses réseau.

Exemple :

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

Activer l'équilibrage de charges ASP

Le mécanisme d'équilibrage de charges ASP permet d'éviter les problèmes suivants :

- Dépassements causés par des pics de trafic imprévus sur les flux
- Dépassements causés par des flux volumineux surchargeant les anneaux de réception d'interfaces spécifiques
- Dépassements causés par des anneaux de réception d'interfaces relativement surchargés, dans lesquels un seul cœur ne peut pas supporter la charge.

L'équilibrage de charges ASP permet à plusieurs cœurs de travailler simultanément sur les paquets qui ont été reçus d'un seul anneau de réception d'interface. Si le système abandonne des paquets et que la sortie de la commande **show cpu** est bien inférieure à 100 %, cette fonctionnalité peut améliorer votre débit si les paquets appartiennent à de nombreuses connexions non liées.

Remarque L'équilibrage de charges ASP est désactivé sur l'ASA virtuel. Avec l'intégration de DPDK (Dataplane Development Kit) dans le chemin de sécurité accéléré (ASP) de l'ASA virtuel, l'ASA virtuel affiche de meilleures performances avec cette fonctionnalité désactivée.

Procédure

Étape 1 Activez et désactivez la commutation automatique de l'équilibrage de charges ASP :

asp load-balance per-packet auto

Étape 2 Activez manuellement l'équilibrage de charges ASP :

asp load-balance per-packet

L'équilibrage de charges ASP est activé jusqu'à ce que vous le désactiviez manuellement, même si vous avez également activé la commande **auto**.

Étape 3 Désactivez manuellement l'équilibrage de charges ASP :

no asp load-balance per-packet

Cette commande s'applique uniquement si vous avez activé manuellement l'équilibrage de charges ASP. Si vous avez également activé la commande **auto**, le système revient à l'activation ou à la désactivation automatique de l'équilibrage de charges ASP.

Supervision du cache DNS

L'ASA fournit un cache local des renseignements DNS à partir des demandes DNS externes qui sont envoyées pour certaines commandes de VPN et de certificat SSL VPN sans client. Chaque demande de traduction DNS est d'abord recherchée dans le cache local. Si la mémoire cache locale contient les informations, l'adresse IP qui en résulte est renvoyée. Si la mémoire cache locale ne peut pas résoudre la demande, une requête DNS est envoyée aux différents serveurs DNS qui ont été configurés. Si un serveur DNS externe résout la demande, l'adresse IP qui en résulte est stockée dans la mémoire cache locale avec son nom d'hôte correspondant.

Consultez la commande suivante pour superviser le cache DNS :

- **show dns-hosts**

  Cette commande affiche le cache DNS, qui comprend les entrées apprises dynamiquement à partir d'un serveur DNS ainsi que le nom et les adresses IP saisis manuellement à l'aide de la commande name.

Historique des paramètres de base

Nom de la caractéristique	Versions de plateforme	Description
Plusieurs groupes de serveurs DNS	9.18(1)	Vous pouvez désormais utiliser plusieurs groupes de serveurs DNS : un groupe est le groupe par défaut, tandis que les autres groupes peuvent être associés à des domaines spécifiques. Une requête DNS qui correspond à un domaine associé à un groupe de serveurs DNS utilisera ce groupe. Par exemple, si vous souhaitez que le trafic destiné aux serveurs internes eng.cisco.com utilise un serveur DNS interne, vous pouvez mapper eng.cisco.com à un groupe DNS interne. Toutes les requêtes DNS qui ne correspondent pas à un mappage de domaine utiliseront le groupe de serveurs DNS par défaut, qui n'a pas de domaine associé. Par exemple, le groupe DefaultDNS peut inclure un serveur DNS public disponible sur l'interface externe. Commandes nouvelles/modifiées : **dns-group-map**, **dns-to-domain**
Serveurs DNS de confiance pour la résolution du domaine d'objet de service réseau.	9.17(1)	Vous pouvez spécifier les serveurs DNS auxquels le système doit faire confiance lors de la résolution des noms de domaine dans les objets de service de réseau. Cette fonctionnalité garantit que toutes les résolutions de noms de domaine DNS acquièrent des adresses IP auprès de sources de confiance. Commandes nouvelles/modifiées : **dns trusted-source**, **show dns trusted-source**
Modification du comportement de la TTL de l'entrée DNS	9.17(1)	Auparavant, la valeur configurée était ajoutée à la TTL existante de chaque entrée (la valeur par défaut était de 1 minute). Désormais, si le délai d'expiration est plus long que la TTL de l'entrée, cette dernière est augmentée jusqu'à la valeur du délai d'expiration de l'entrée. Si la TTL est plus longue que le délai d'expiration, la valeur du délai d'expiration est ignorée; dans ce cas, aucun délai supplémentaire n'est ajouté à la TTL. Commandes nouvelles ou modifiées : **expire-entry-timer minutes**

Nom de la caractéristique	Versions de plateforme	Description
Exigences relatives à l'utilisateur local et au mot de passe d'activation	9.17(1)	Pour les utilisateurs locaux et le mot de passe d'activation, les exigences de mot de passe suivantes ont été ajoutées : • Longueur du mot de passe : au moins 8 caractères. Auparavant, le minimum était de 3 caractères. • Caractères répétitifs et séquentiels : trois caractères ASCII ou plus consécutifs ne sont pas autorisés. Par exemple, les mots de passe suivants seront refusés : • **abc**utilisateur1 • utilisateur**543** • utilisateur**aaaa** • utilisateur2**666** Commandes nouvelles/modifiées : **enable password**, **username**
Prise en charge NTPv4	9.14(1)	L'ASA prend désormais en charge NTPv4. Aucune commande modifiée.
Algorithmes d'authentification NTP supplémentaires	9.13(1)	Auparavant, seul MD5 était pris en charge pour l'authentification NTP. L'ASA prend désormais en charge les algorithmes suivants : • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC Commandes nouvelles ou modifiées : **ntp authentication-key**
Prise en charge de NTP sur IPv6	9.12(1)	Vous pouvez maintenant spécifier une adresse IPv6 pour le serveur NTP. Commandes nouvelles ou modifiées : **ntp server**

Nom de la caractéristique	Versions de plateforme	Description
Le changement de mot de passe **enable** est maintenant requis lors de la connexion	9.12(1)	Le mot de passe par défaut **enable** est vide. Lorsque vous essayez d'accéder en mode d'exécution privilégié sur l'ASA, vous devez désormais modifier le mot de passe pour une valeur de 3 à 127 caractères. Vous ne pouvez pas le garder vide. La commande **no enable password** n'est plus prise en charge. Au niveau de l'interface de ligne de commande, vous pouvez accéder au mode d'exécution privilégié à l'aide des commandes **enable**, **login** (avec un utilisateur de niveau de privilège 2+), ou d'une session SSH ou Telnet lorsque vous activez **aaa authorization exec auto-enable**. Toutes ces méthodes nécessitent que vous définissiez le mot de passe d'activation. Cette exigence de changement de mot de passe n'est pas appliquée pour les connexions ASDM. Dans ASDM, par défaut, vous pouvez vous connecter sans nom d'utilisateur et avec le mot de passe **enable**. Commandes nouvelles ou modifiées : **enable password**
L'équilibrage de charges ASP est désactivé sur l'ASA virtuel	9.10(1)	Avec la récente intégration de DPDK (Dataplane Development Kit) dans le chemin de sécurité accéléré (ASP) de l'ASA virtuel, l'ASA virtuel affiche de meilleures performances avec cette fonctionnalité désactivée.
L'équilibrage automatique de la charge ASP est désormais pris en charge pour l'ASA virtuel.	9.8(1)	Auparavant, vous pouviez uniquement activer et désactiver manuellement l'équilibrage de charges ASP. Nous avons modifié la commande suivante : **asp load-balance per-packet auto**
Hachage PBKDF2 pour tous les mots de passe locaux **username** et **enable**	9.7(1)	Les mots de passe locaux **username** et **enable** de toutes les longueurs sont stockés dans la configuration à l'aide du hachage PBKDF2 (Password-Based Key Derivation Function 2) à l'aide de SHA-512. Auparavant, les mots de passe de 32 caractères et moins utilisaient la méthode de hachage basée sur MD5. Les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Consultez le chapitre « Logiciels et configurations » du Guide de configuration des opérations générales pour connaître les lignes directrices relatives à la rétrogradation. Nous avons modifié les commandes suivantes : **enable, username**
Prise en charge des alimentations doubles pour l'ISA 3000	9.6(1)	Pour les alimentations doubles dans l'ISA 3000, vous pouvez établir des alimentations doubles comme la configuration attendue dans le système d'exploitation ASA. En cas de défaillance d'une alimentation, l'ASA émet une alarme. Par défaut, l'ASA s'attend à une seule alimentation et n'émettra pas d'alarme tant qu'il dispose d'une alimentation opérationnelle. Nous avons introduit la commande suivante : **power-supply dual**
Prise en charge de mots de passe plus longs pour les mots de passe locaux **username** et **enable** (jusqu'à 127 caractères)	9.6(1)	Vous pouvez désormais créer des mots de passe **username** et **enable** locaux jusqu'à 127 caractères (l'ancienne limite était de 32). Lorsque vous créez un mot de passe de plus de 32 caractères, il est stocké dans la configuration à l'aide d'un hachage PBCDF2 (Password-Based Key Derivation Function 2). Les mots de passe plus courts continuent d'utiliser la méthode de hachage basée sur MD5. Nous avons modifié les commandes suivantes : **enable, username**

Nom de la caractéristique	Versions de plateforme	Description
contournement matériel ISA 3000	9.4(1.225)	L'ISA 3000 prend en charge une fonction de contournement matériel pour permettre au trafic de continuer à circuler dans l'appareil en cas de perte d'alimentation. Nous avons introduit les commandes suivantes : **hardware-bypass, hardware-bypass manual, hardware-bypass boot-delay, show hardware-bypass** *Cette fonctionnalité n'est pas disponible dans la version 9.5(1).*
Équilibrage de charges ASP automatique	9.3(2)	Vous pouvez maintenant activer le basculement automatique vers la fonction d'équilibrage de charges ASP. **Remarque** La fonction automatique n'est pas prise en charge sur l'ASA virtuel; seules l'activation et la désactivation manuelles sont prises en charge. Nous avons introduit la commande suivante : **asp load-balance per-packet auto**.
Suppression du mot de passe Telnet par défaut	9.0(2)/9.1(2)	Pour améliorer la sécurité de l'accès de gestion à l'ASA, le mot de passe de connexion par défaut pour Telnet a été supprimé; vous devez définir manuellement le mot de passe avant de pouvoir vous connecter en utilisant Telnet. **Remarque** Le mot de passe de connexion n'est utilisé pour Telnet que si vous ne configurez pas l'authentification de l'utilisateur Telnet (la commande **aaa authentication telnet console**). Auparavant, lorsque vous effaciez le mot de passe, l'ASA rétablissait le mot de passe par défaut « cisco ». Maintenant, lorsque vous effacez le mot de passe, le mot de passe est supprimé. Le mot de passe de connexion est également utilisé pour les sessions Telnet, du commutateur à l'ASASM (voir la commande **session**). Pour l'accès initial à l'ASASM, vous devez utiliser la commande **service-module session**, jusqu'à ce que vous définissiez un mot de passe de connexion. Nous avons modifié la commande suivante : **password**
Visibilité du chiffrement des mots de passe	v 8.4(1)	Nous avons modifié la commande **show password encryption**.
Phrase secrète principale	8.3(1)	Nous avons introduit cette fonctionnalité. La phrase secrète principale vous permet de stocker en toute sécurité les mots de passe en texte brut dans un format chiffré et fournit une clé utilisée pour chiffrer ou masquer tous les mots de passe de manière universelle, sans modifier aucune fonctionnalité. Nous avons introduit les commandes suivantes : **key config-key password-encryption**, **password encryption aes**, **clear configure password encryption aes**, **show running-config password encryption aes, show password encryption**



CHAPITRE 24

Services DHCP et DDNS

Ce chapitre décrit comment configurer le serveur DHCP ou le relais DHCP, ainsi que les méthodes de mise à jour du DNS dynamique (DDNS).

- À propos des services DHCP et DDNS, à la page 857
- Lignes directrices pour les services DHCP et DDNS, à la page 859
- Configurer le serveur DHCP, à la page 861
- Configurer les agents de relais DHCP., à la page 867
- Configuration du DNS dynamique, à la page 870
- Supervision des services DHCP et DDNS, à la page 876
- Historique des services DHCP et DDNS, à la page 881

À propos des services DHCP et DDNS

Les rubriques suivantes décrivent le serveur DHCP, l'agent de relais DHCP et la mise à jour DDNS.

À propos du serveur DHCPv4

DHCP fournit des paramètres de configuration réseau, tels que des adresses IP, aux clients DHCP. Le périphérique ASA peut fournir un serveur DHCP aux clients DHCP connectés aux interfaces ASA. Le serveur DHCP fournit des paramètres de configuration réseau directement aux clients DHCP.

Un client DHCP IPv4 utilise une adresse de diffusion plutôt qu'une adresse de multidiffusion pour atteindre le serveur. Le client DHCP est à l'écoute des messages sur le port UDP 68; le serveur DHCP est à l'écoute des messages sur le port UDP 67.

Options de DHCP

DHCP fournit une structure pour la transmission des informations de configuration aux hôtes sur un réseau TCP/IP. Les paramètres de configuration sont transportés dans des éléments étiquetés qui sont stockés dans le champ Options du message DHCP. Les données sont également appelées options. Les renseignements sur le fournisseur sont également stockés dans Options, et tous les postes d'informations sur le fournisseur peuvent être utilisés comme options DHCP.

Par exemple, les téléphones IP Cisco téléchargent leur configuration à partir d'un serveur TFTP. Lorsqu'un téléphone IP Cisco démarre, si l'adresse IP et l'adresse IP du serveur TFTP ne sont pas préconfigurées, il envoie une demande avec l'option 150 ou 66 au serveur DHCP pour obtenir cette information.

- L’option 150 de DHCP fournit les adresses IP d’une liste de serveurs TFTP.
- L’option DHCP 66 fournit l’adresse IP ou le nom d’hôte d’un seul serveur TFTP.
- L’option 3 de DHCP définit la voie de routage par défaut.

Une seule demande peut inclure les deux options 150 et 66. Dans ce cas, le serveur DHCP fournit des valeurs pour les deux options dans la réponse si elles sont déjà configurées sur l’ASA.

Vous pouvez utiliser les options DHCP avancées pour fournir les paramètres DNS, WINS et de nom de domaine aux clients DHCP. L’option DHCP 15 est utilisée pour le suffixe de domaine DNS. Vous pouvez également utiliser le paramètre de configuration automatique DHCP pour obtenir ces valeurs ou les définir manuellement. Lorsque vous utilisez plusieurs méthodes pour définir ces informations, elles sont transmises aux clients DHCP dans l'ordre suivant :

1. Paramètres configurés manuellement.
2. Paramètres des options DHCP avancées
3. Paramètres de configuration automatique de DHCP.

Par exemple, vous pouvez définir manuellement le nom de domaine que vous souhaitez que les clients DHCP reçoivent, puis activer la configuration automatique de DHCP. Bien que la configuration automatique de DHCP découvre le domaine ainsi que les serveurs DNS et WINS, le nom de domaine défini manuellement est transmis aux clients DHCP avec les noms de serveurs DNS et WINS découverts, car le nom de domaine découvert par le processus de configuration automatique de DHCP est remplacé par l’ domaine défini.

À propos du serveur sans état DHCPv6

Pour les clients qui utilisent la configuration automatique des adresses sans état (SLAAC) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6, à la page 781), vous pouvez configurer les ASA pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu’ils envoient des paquets de demande d’information (IR) à l’ASA. Le ASA accepte uniquement les paquets IR et n’affecte pas d’adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d’autres termes, en fonction du préfixe que ASA a reçu à l’aide de la délégation de préfixe.

À propos de l'agent relais DHCP

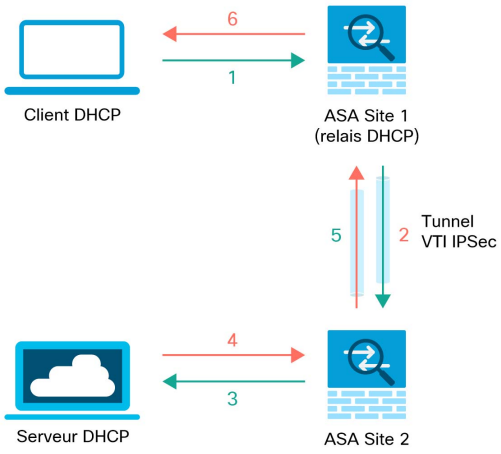
Vous pouvez configurer un agent de relais DHCP pour transférer les demandes DHCP reçues sur une interface vers un ou plusieurs serveurs DHCP. Les clients DHCP utilisent les diffusions UDP pour envoyer leurs premiers messages DHCPDISCOVER, car ils ne disposent pas d'informations sur le réseau auquel ils sont connectés. Si le client se trouve sur un segment de réseau qui n’inclut pas de serveur, les diffusions UDP ne sont normalement pas transférées par le périphérique ASA, car il ne transfère pas le trafic de diffusion. L’agent de relais DHCP vous permet de configurer l’interface du ASA qui reçoit les diffusions pour transférer les demandes DHCP vers un serveur DHCP qui est disponible via un autre périphérique.

Prise en charge du serveur relais DHCP sur VTI

Vous pouvez configurer un agent de relais DHCP sur une interface ASA pour recevoir et transférer des messages DHCP entre un client DHCP et un serveur DHCP. Cependant, un serveur de relais DHCP pour transférer des messages par l’intermédiaire d’une interface logique n’était pas pris en charge.

La figure suivante montre le processus de découverte du client DHCP et du serveur DHCP qui utilise le relais DHCP sur le VPN VTI. L'agent de relais DHCP, configuré sur l'interface VTI du site 1 de l'ASA, reçoit le paquet DHCPDISCOVER du client DHCP et envoie le paquet par le tunnel VTI. Le site 2 de l'ASA transmet le paquet DHCPDISCOVER au serveur DHCP. Le serveur DHCP répond par un DHCPOFFER au site 2 de l'ASA. L'ASA du site 2 l'envoie au relais DHCP (site 1 de l'ASA), qui l'envoie au client DHCP.

Illustration 65 : Serveur relais DHCP sur VTI



La même procédure est suivie pour les exigences DHCPREQUEST et DHCPACK/NACK.

Lignes directrices pour les services DHCP et DDNS

Cette section comprend des directives et des limites que vous devez vérifier avant de configurer les services DHCP et DDNS.

Mode contextuel

- Le serveur sans état DHCPv6 n'est pas pris en charge en mode contexte multiple.

Mode pare-feu

- Le relais DHCP n'est pas pris en charge en mode transparent de pare-feu ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.
- Le serveur DHCP est pris en charge en mode de pare-feu transparent sur une interface de membre de groupe de ponts. En mode routé, le serveur DHCP est pris en charge sur l'interface BVI, pas sur l'interface des membres du groupe de ponts. Les BVI doivent avoir un nom pour que le serveur DHCP puisse fonctionner.
- DDNS n'est pas pris en charge en mode de pare -feu transparent ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.
- Le serveur sans état DHCPv6 n'est pas pris en charge en mode de pare-feu transparent ou en mode routé sur l'interface de BVI ou de membre du groupe de ponts.

Mise en grappe

- Le serveur sans état DHCPv6 n'est pas pris en charge par la mise en grappe.

IPv6

Prend en charge IPv6 pour le serveur sans état DHCP et le relais DHCP.

Serveur DHCPv4

- L'ensemble DHCP disponible maximal est de 256 adresses.
- Vous pouvez configurer un serveur DHCP sur n'importe quelle interface avec un nom et une adresse IP, comme une interface physique, une sous-interface ou une BVI en mode routé.
- Vous ne pouvez configurer qu'un seul serveur DHCP sur chaque interface. Chaque interface peut avoir son propre ensemble d'adresses à utiliser. Cependant, les autres paramètres DHCP, tels que les serveurs DNS, le nom de domaine, les options, le délai de ping et les serveurs WINS, sont configurés globalement et utilisés par le serveur DHCP sur toutes les interfaces.
- Vous ne pouvez pas configurer une interface en tant que client DHCP si un serveur DHCP est également activé sur cette interface; vous devez utiliser une adresse IP statique.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- Vous pouvez réserver une adresse DHCP pour une interface. ASA attribue une adresse spécifique de l'ensemble d'adresses à un client DHCP en fonction de l'adresse MAC du client.
- L'ASA ne prend pas en charge les serveurs DHCP QIP pour une utilisation avec le service mandataire DHCP.
- Le serveur DHCP ne prend pas en charge les demandes BOOTP.

Serveur PD DHCPv6

Le serveur sans état DHCPv6 ne peut pas être configuré sur une interface où l'adresse DHCPv6, le client de délégation de préfixe ou le relais DHCPv6 est configuré.

Relais DHCP

- Vous pouvez configurer un maximum de 10 serveurs relais DHCPv4, avec un maximum de 4 serveurs par interface.
- Vous pouvez configurer un maximum de 10 serveurs relais DHCPv6. Les serveurs propres à une interface pour IPv6 ne sont pas pris en charge.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- Les services de relais DHCP ne sont pas offerts dans le mode transparent du pare-feu ou le mode routé sur l'interface des BVI ou celle des membres du groupe de ponts. Vous pouvez, cependant, autoriser le trafic DHCP en utilisant une règle d'accès. Pour autoriser les demandes et les réponses DHCP par l'intermédiaire du ASA, vous devez configurer deux règles d'accès, une qui autorise les demandes DHCP

de l'interface interne vers l'extérieur (port de destination d'UDP 67) et une qui autorise les réponses du serveur de l'autre côté (port de destination UDP 68).

- Pour IPv4, les clients doivent être connectés directement à ASA et ne peuvent pas envoyer de demandes par un autre agent de relais ou un routeur. Pour IPv6, ASA prend en charge les paquets d'un autre serveur de relais.
- Les clients DHCP doivent se trouver sur des interfaces différentes des serveurs DHCP vers lesquels ASA relaye les demandes.
- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone de trafic.

Service DDNS

Le DDNS du pare-feu prend uniquement en charge le service DynDNS. Par conséquent, assurez-vous que le DDNS est configuré avec l'URL de mise à jour dans la syntaxe suivante :

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**.

Configurer le serveur DHCP

Cette section décrit comment configurer un serveur DHCP fourni par l'ASA.

Procédure

Étape 1 Activer le serveur DHCPv4, à la page 861.
Étape 2 Configurer les options DHCPv4 avancées, à la page 863.
Étape 3 Configurer le serveur sans état DHCPv6, à la page 865.

Activer le serveur DHCPv4

Pour activer le serveur DHCP sur une interface ASA, procédez comme suit :

Procédure

Étape 1 Créez un ensemble d'adresses DHCP pour une interface. L'ASA attribue à un client une des adresses de cet ensemble à utiliser pendant une période donnée. Ces adresses sont les adresses locales et non traduites pour le réseau connecté directement.

dhcpd address *ip_address_start-ip_address_end if_name*

Exemple :

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

L'ensemble d'adresses doit se trouver sur le même sous-réseau que l'interface ASA. En mode transparent, spécifiez une interface de membres de groupe de ponts. En mode routé, spécifiez une interface routée ou un BVI; ne spécifiez pas l'interface des membres du groupe de ponts.

Étape 2 (Facultatif) (Mode routé) Configurez automatiquement les valeurs DNS, WINS et des noms de domaine obtenues à partir d'une interface exécutant un client DHCP ou PPPoE, ou à partir d'un serveur VPN.

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

Exemple :

```
ciscoasa(config)# dhcpd auto_config outside interface inside
```

Si vous spécifiez les paramètres DNS, WINS ou des noms de domaine à l'aide des commandes suivantes, ils remplacent les paramètres obtenus par la configuration automatique.

Étape 3 (Facultatif) Réservez une adresse DHCP pour un client. L'ASA attribue une adresse spécifique de l'ensemble d'adresses configué à un client DHCP en fonction de l'adresse MAC du client.

dhcpd reserve-address *ip_address mac_address if_name*

Exemple :

```
ciscoasa(config)# dhcpd reserve-address 10.0.1.109 030c.f142.4cde inside
```

L'adresse réservée doit provenir de l'ensemble d'adresses configuré, et l'ensemble d'adresses doit se trouver sur le même sous-réseau que l'interface ASA. En mode transparent, spécifiez une interface de membres de groupe de ponts. En mode routé, spécifiez une interface routée ou un BVI; ne spécifiez pas l'interface des membres du groupe de ponts.

Étape 4 (Facultatif) Spécifiez la ou les adresses IP du ou des serveurs DNS.

dhcpd dns *dns1* [*dns2*]

Exemple :

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

Étape 5 (Facultatif) Spécifiez la ou les adresses IP du ou des serveurs WINS. Vous pouvez spécifier jusqu'à deux serveurs WINS.

dhcpd wins *wins1* [*wins2*]

Exemple :

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

Étape 6 (Facultatif) Modifiez la durée du bail locatif à accorder au client. La durée du bail locatif équivaut à la durée en secondes pendant laquelle le client peut utiliser l'adresse IP qui lui a été attribuée avant l'expiration du bail. Saisissez une valeur de 0 à 1 048 575. La valeur par défaut est de 3 600 secondes.

dhcpd lease *lease_length*

Exemple :

```
ciscoasa(config)# dhcpd lease 3000
```

Étape 7 (Facultatif) Configurez le nom de domaine.

dhcpd domain *domain_name*

Exemple :

```
ciscoasa(config)# dhcpd domain example.com
```

Étape 8 (Facultatif) Configurez la valeur du délai d'expiration de l'envoi d'un message Ping DHCP pour les paquets ICMP. Pour éviter les conflits d'adresses, l'ASA envoie deux paquets Ping ICMP à une adresse avant d'affecter cette adresse à un client DHCP. La valeur par défaut est de 50 millisecondes.

dhcpd ping timeout *milliseconds*

Exemple :

```
ciscoasa(config)# dhcpd ping timeout 20
```

Étape 9 Définissez une passerelle par défaut qui est envoyée aux clients DHCP. Pour le mode routé, si vous n'utilisez pas la commande **dhcpd option 3 ip**, l'ASA envoie l'adresse IP de l'interface activée pour le serveur DHCP comme passerelle par défaut. Pour le mode transparent, vous devez définir **dhcpd option 3 ip** si vous souhaitez définir une passerelle par défaut; l'ASA lui-même ne peut pas servir de passerelle par défaut.

dhcpd option 3 ip *gateway_ip*

Exemple :

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

Étape 10 Activez le démon DHCP dans l'ASA pour écouter les demandes des clients DHCP sur l'interface activée.

dhcpd enable *interface_name*

Exemple :

```
ciscoasa(config)# dhcpd enable inside
```

Spécifiez la même interface que la plage **dhcpd address**.

Configurer les options DHCPv4 avancées

L'ASA prend en charge les options DHCP répertoriées dans RFC 2132, RFC 2562 et RFC 5510 pour l'envoi de renseignements. Toutes les options DHCP (1 à 255) sont prises en charge, à l'exception des 1, 12, 50 à 54,58 à 59, 61, 67 et 82.

Procédure

Étape 1 Configurez une option DHCP qui renvoie une ou deux adresses IP :

dhcpd option *code* **ip** *addr_1* [*addr_2*]

Exemple :

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
ciscoasa(config)# dhcpd option 3 ip 10.10.1.10
```

L'option 150 fournit l'adresse IP ou les noms d'un ou de deux serveurs TFTP à utiliser avec les téléphones IP Cisco. L'option 3 définit le routage par défaut pour les téléphones IP Cisco.

Étape 2 Configurez une option DHCP qui renvoie une chaîne de texte :

dhcpd option *code* **ascii** *text*

Exemple :

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

L'option 66 fournit l'adresse IP ou le nom d'un serveur TFTP à utiliser avec les téléphones IP Cisco.

Étape 3 Configurez une option DHCP qui renvoie une valeur hexadécimale.

dhcpd option code hex *value*

Exemple :

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

Remarque
L'ASA ne vérifie pas que le type et la valeur d'option que vous fournissez correspondent au type et à la valeur attendus pour le code d'option, comme défini dans la RFC 2132. Par exemple, vous pouvez saisir la commande **dhcpd option 46 ascii hello** et l'ASA accepte la configuration, bien que l'option 46 soit définie dans la RFC 2132 pour s'attendre à une valeur hexadécimale à un seul chiffre. Pour en savoir plus sur les codes d'option, les types associés et les valeurs attendues, consultez la RFC 2132.

Le tableau suivant présente les options DHCP qui ne sont pas prises en charge par la commande **dhcpd option** .

Tableau 32 : Options DHCP non prises en charge

Code d'option	Description
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS

Code d'option	Description
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

Configurer le serveur sans état DHCPv6

Pour les clients qui utilisent SLAAC (StateLess Address Auto Configuration) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6, à la page 781), vous pouvez configurer l'ASA pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresses aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que l'ASA a reçu à l'aide de la délégation de préfixe.

Avant de commencer

Cette fonctionnalité n'est prise en charge qu'en mode routé simple. Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe.

Procédure

Étape 1 Configurez l'ensemble d'adresses DHCP IPv6 qui contient les informations que vous souhaitez que le serveur DHCPv6 fournisse :

ipv6 dhcp pool *pool_name*

Exemple :

```
ciscoasa(config)# ipv6 dhcp pool Inside-Pool
ciscoasa(config)#
```

Vous pouvez configurer des ensembles distincts pour chaque interface si vous le souhaitez, ou utiliser le même ensemble sur plusieurs interfaces.

Étape 2 Configurez un ou plusieurs des paramètres suivants à fournir aux clients dans les réponses aux messages IR :

dns-server *dns_ipv6_address*

domain-name *domain_name*

nis address *nis_ipv6_address*

nis domain-name *nis_domain_name*

nisp address *nisp_ipv6_address*

nisp domain-name *nisp_domain_name*

sip address *sip_ipv6_address*

sip domain-name *sip_domain_name*

sntp address *sntp_ipv6_address*

import {[**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**]}

Exemple :

```
ciscoasa(config-dhcpv6)# domain-name example.com
ciscoasa(config-dhcpv6)# import dns-server
```

La commande **import** utilise un ou plusieurs paramètres que l'ASA a obtenus du serveur DHCPv6 sur l'interface client de délégation de préfixe. Vous pouvez combiner des paramètres configurés manuellement avec des paramètres importés; cependant, vous ne pouvez pas configurer le même paramètre manuellement et dans la commande **import**.

Étape 3 Passez en mode de configuration d'interface pour l'interface sur laquelle vous souhaitez que l'ASA écoute les messages IP :

interface *ID*

Exemple :

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

Étape 4 Activer le serveur DHCPv6 :

ipv6 dhcp server *pool_name*

Exemple :

```
ciscoasa(config-if)# ipv6 dhcp server Inside-Pool
ciscoasa(config-if)#
```

Étape 5 Configurez l'annonce de routeur pour informer les clients du SLAAC du serveur DHCPv6 :

ipv6 nd other-config-flag

Cet indicateur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des informations supplémentaires de DHCPv6, telles que l'adresse du serveur DNS.

Exemple

Dans l'exemple suivant, deux groupes DHCP IPv6 sont créés et le serveur DHCPv6 est activé sur deux interfaces :

```
ipv6 dhcp pool Eng-Pool
  domain-name eng.example.com
  import dns-server
ipv6 dhcp pool IT-Pool
  domain-name it.example.com
  import dns-server
interface gigabitethernet 0/0
  ipv6 address dhcp setroute default
  ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ipv6 dhcp server Eng-Pool
  ipv6 nd other-config-flag
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
  ipv6 dhcp server IT-Pool
  ipv6 nd other-config-flag
```

Configurer les agents de relais DHCP.

Lorsqu'une requête DHCP entre dans une interface, les serveurs DHCP auxquels l'ASA relaye la requête dépendent de votre configuration. Vous pouvez configurer les types de serveurs suivants :

- Serveurs DHCP spécifiques à l'interface : lorsqu'une requête DHCP entre dans une interface particulière, l'ASA ne relaye la requête qu'aux serveurs spécifiques à l'interface.
- Serveurs DHCP globaux : lorsqu'une requête DHCP entre dans une interface qui n'a pas de serveurs spécifiques à l'interface configurés, l'ASA relaye la requête à tous les serveurs globaux. Si l'interface comporte des serveurs propres à une interface, les serveurs globaux ne sont pas utilisés.

Configurer l'agent de relais DHCPv4

Lorsqu'une requête DHCP entre dans une interface, l'ASA la relaye au serveur DHCP.

Procédure

Étape 1 Effectuez l'une des opérations suivantes ou les deux :

- Spécifiez une adresse IP globale de serveur DHCP et l'interface par laquelle il est accessible.

  dhcprelay server *ip_address if_name*

Exemple :

```
ciscoasa(config)# dhcprelay server 209.165.201.5 outside
ciscoasa(config)# dhcprelay server 209.165.201.8 outside
ciscoasa(config)# dhcprelay server 209.165.202.150 it
```

- Spécifiez l'ID de l'interface connectée au réseau client DHCP et l'adresse IP du serveur DHCP à utiliser pour les requêtes DHCP qui accèdent à cette interface.

```
interface interface_id
  dhcprelay server ip_address
```

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config)# dhcprelay server 209.165.201.6
ciscoasa(config)# dhcprelay server 209.165.201.7
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config)# dhcprelay server 209.165.202.155
ciscoasa(config)# dhcprelay server 209.165.202.156
```

Notez que vous ne spécifiez pas l'interface de sortie pour les requêtes, comme dans la commande globale **dhcprelay server**; au lieu de cela, l'ASA utilise la table de routage pour déterminer l'interface de sortie.

Étape 2 Activez le service de relais DHCP sur l'interface connectée aux clients DHCP. Vous pouvez activer le relais DHCP sur plusieurs interfaces.

dhcprelay enable *interface*

Exemple :

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

Étape 3 (Facultatif) Définissez le nombre de secondes autorisées pour le traitement de l'adresse de relais DHCP.

dhcprelay timeout *seconds*

Exemple :

```
ciscoasa(config)# dhcprelay timeout 25
```

Étape 4 (Facultatif) Modifiez la première adresse de routeur par défaut dans le paquet envoyé par le serveur DHCP pour qu'elle corresponde à l'adresse de l'interface ASA.

dhcprelay setroute *interface_name*

Exemple :

```
ciscoasa(config)# dhcprelay setroute inside
```

Cette action permet au client de configurer sa route par défaut pour qu'elle pointe vers l'ASA, même si le serveur DHCP spécifie un routeur différent.

S'il n'y a pas d'option de routeur par défaut dans le paquet, l'ASA en ajoute une contenant l'adresse de l'interface.

Étape 5 (Facultatif) Configurez les interfaces en tant qu'interfaces de confiance. Effectuez l'une des opérations suivantes :

- Spécifiez une interface client DHCP en laquelle vous souhaitez avoir confiance :

```
interface interface_id
  dhcprelay information trusted
```

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# dhcprelay information trusted
```

Vous pouvez configurer des interfaces en tant qu'interfaces de confiance pour conserver l'option 82 de DHCP. L'option 82 DHCP est utilisée par les commutateurs et les routeurs en aval pour la surveillance DHCP et la protection source IP. Normalement, si l'agent de relais DHCP ASA reçoit un paquet DHCP avec l'option 82 déjà définie, mais que le champ giaddr (qui spécifie l'adresse de l'agent de relais DHCP définie par ce dernier avant de transmettre le paquet au serveur) est réglé sur 0, l'ASA supprimera ce paquet par défaut. Vous pouvez désormais conserver l'option 82 et transférer le paquet en identifiant une interface comme interface de confiance.

- Configurez toutes les interfaces client comme de confiance :

dhcprelay information trust-all

Exemple :

```
ciscoasa(config)# dhcprelay information trust-all
```

Configurer l'agent de relais DHCPv6

Lorsqu'une requête DHCPv6 entre dans une interface, l'ASA la relaye à tous les serveurs globaux DHCPv6.

Procédure

Étape 1 Spécifiez l'adresse de destination du serveur DHCP IPv6 à laquelle les messages des clients sont transférés.

ipv6 dhcprelay server *ipv6_address* [*interface*]

Exemple :

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

L'argument *ipv6-address* peut être une adresse de monodiffusion à portée de liaison, une adresse de multidiffusion, une adresse de monodiffusion à portée de site ou une adresse IPv6 globale. Les adresses de multidiffusion non spécifiées, de boucle avec retour et locales au nœud ne sont pas autorisées comme destination de relais. L'argument *interface* facultatif spécifie l'interface de sortie d'une destination. Les messages des clients sont acheminés à l'adresse de destination par la liaison à laquelle l'interface de sortie est connectée. Si l'adresse spécifiée est une adresse à portée de liaison, vous devez indiquer l'interface.

Étape 2 Activez le service de relais DHCPv6 sur une interface.

ipv6 dhcprelay enable *interface*

Exemple :

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Étape 3 (Facultatif) Précisez la durée en secondes autorisée pour les réponses du serveur DHCPv6 à transmettre au client DHCPv6 via la liaison de relais pour la gestion des adresses de relais.

ipv6 dhcprelay timeout *seconds*

Exemple :

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

Les valeurs valides pour l'argument *seconds* sont comprises entre 1 et 3600. La valeur par défaut est de 60 secondes.

Configuration du DNS dynamique

Lorsqu'une interface utilise l'adressage IP DHCP, l'adresse IP attribuée peut changer lors du renouvellement du bail DHCP. Lorsque l'interface doit être accessible à l'aide d'un nom de domaine complet (FQDN), le changement d'adresse IP peut rendre périmés les enregistrements de ressources du serveur DNS. Le DNS dynamique (DDNS) fournit un mécanisme pour mettre à jour les programmes de routage du DNS chaque fois que l'adresse IP ou le nom d'hôte change. Vous pouvez également utiliser DDNS pour les adresses IP statiques ou PPPoE.

DDNS met à jour les réflecteurs de routage suivants sur le serveur DNS : le RR A comprend le mappage nom-adresse IP, tandis que le RR PTR mappe les adresses aux noms.

L'ASA prend en charge les méthodes de mise à jour DDNS suivantes :

- DDNS standard : la méthode de mise à jour DDNS standard est définie par la RFC 2136.

  Avec cette méthode, l'ASA et le serveur DHCP utilisent les requêtes DNS pour mettre à jour les taux de renouvellement (RR) DNS. L'ASA ou le serveur DHCP envoie une requête DNS à son serveur DNS local pour obtenir des renseignements sur le nom d'hôte et, en fonction de la réponse, détermine le serveur DNS principal qui possède les RR. L'ASA ou le serveur DHCP envoie ensuite une demande de mise à jour directement au serveur DNS principal. Consultez les scénarios typiques suivants.

  - L'ASA met à jour le RR de A et le serveur DHCP met à jour le RR des PTR.

En règle générale, l'ASA « possède » le RR de A, tandis que le serveur DHCP « possède » le taux de renouvellement (RR) PTR, de sorte que les deux entités doivent demander les mises à jour séparément. Lorsque l'adresse IP ou le nom d'hôte change, l'ASA envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR du PTR.

- Le serveur DHCP met à jour les taux de renouvellement A et PTR.

  Utilisez ce scénario si l'ASA n'a pas l'autorité pour mettre à jour le RR de A. Lorsque l'adresse IP ou le nom d'hôte change, l'ASA envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR A et PTR.

Vous pouvez configurer différentes propriétés en fonction de vos besoins en matière de sécurité et des exigences du serveur DNS principal. Par exemple, pour une adresse statique, l'ASA doit être propriétaire des mises à jour pour les deux enregistrements.

- Web : la méthode de mise à jour Web utilise la spécification de l'API distante DynDNS. (https://help.dyn.com/remote-access-api/).

  Avec cette méthode, lorsque l'adresse IP ou le nom d'hôte change, l'ASA envoie une requête HTTP directement à un fournisseur DNS auprès duquel vous avez un compte.

Remarque DDNS n'est pas pris en charge sur les interfaces BVI ou de membre du groupe de ponts.

Avant de commencer

- Configurez un serveur DNS sur **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**. Consultez Configurer des serveurs DNS, à la page 844.
- Configurez le nom d'hôte et le nom de domaine du périphérique dans **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)**. Consultez Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet, à la page 831. Si vous ne spécifiez pas de nom d'hôte par interface, le nom d'hôte du périphérique est utilisé. Si vous ne spécifiez pas de FQDN, pour l'adressage IP statique ou PPPoE, le nom de domaine du système ou le nom de domaine du serveur DNS est ajouté au nom d'hôte.

Procédure

Étape 1 Méthode standard DDNS : configurez une méthode de mise à jour DDNS pour activer les requêtes DNS de l'ASA.

Vous n'avez pas besoin de configurer une méthode de mise à jour DDNS si le serveur DHCP effectue toutes les demandes.

a) Créez une méthode de mise à jour.

ddns update method *name*

Exemple :

```
ciscoasa(config)# ddns update method ddns1
ciscoasa(DDNS-update-method)#
```

b) Spécifiez la méthode DDNS standard.

ddns [**both**]

Par défaut, l'ASA met uniquement à jour le RR A. Utilisez ce paramètre si vous souhaitez que le serveur DHCP mette à jour le RR des PTR. Si vous souhaitez que l'ASA mette à jour le RR A et PTR, spécifiez **both**. Utilisez le mot clé **both** pour les adresses IP statiques ou PPPoE.

Exemple :

```
ciscoasa(DDNS-update-method)# ddns
```

c) (Facultatif) Configurez l'intervalle de mise à jour entre les requêtes DNS.

interval maximum *days hours minutes seconds*

Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres *days* (jours) (0-364), *hours* (heures), *minutes* et *seconds* (secondes).

Exemple :

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

d) Associez cette méthode à une interface. Consultez Étape 3, à la page 873.

Étape 2 Méthode Web : configurez une méthode de mise à jour DDNS pour activer les demandes de mise à jour HTTP à partir de l'ASA.

a) Créez une méthode de mise à jour.

ddns update method *name*

Exemple :

```
ciscoasa(config)# ddns update method web1
ciscoasa(DDNS-update-method)#
```

b) Spécifiez le nom d'identité de référence pour valider l'identité du certificat du serveur DDNS. L'ASA tente de trouver une correspondance de nom d'hôte. Si l'hôte ne peut être résolu ou si aucune correspondance n'est trouvée, la connexion est interrompue.

Exemple :

```
ciscoasa(DDNS-update-method)# web reference-identity dyndns
```

c) Spécifiez la méthode Web et l'URL de mise à jour.

web update-url https://*username (nom d'utilisateur)***:***password (mot de passe)***@***provider-domain (domaine du fournisseur)*/*path (chemin)***?hostname=<h>&myip=<a>**

Avant de saisir le point d'interrogation (?), appuyez simultanément sur les touches Ctrl et v de votre clavier. Cela vous permettra de saisir le caractère ? sans que le logiciel l'interprète comme une requête d'aide.

Exemple :

```
ciscoasa(DDNS-update-method)#
web update-url
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
```

d) (Facultatif) Spécifiez les types d'adresses (IPv4 ou IPv6) que vous souhaitez mettre à jour.

Par défaut, l'ASA met à jour toutes les adresses IPv4 et IPv6. Si vous souhaitez limiter les adresses, saisissez la commande suivante.

web update-type {**ipv4** | **ipv6** [**all**] | **both** [**all**]}

- **both all** : (par défaut) met à jour toutes les adresses IPv4 et IPv6.
- **both** : met à jour l'adresse IPv4 et la dernière adresse IPv6.
- **ipv4** : met à jour uniquement l'adresse IPv4.
- **ipv6** : met à jour uniquement la dernière adresse IPv6.
- **ipv6 all** : met à jour toutes les adresses IPv6.

Exemple :

```
ciscoasa(DDNS-update-method)# web update-type ipv4
```

e) (Facultatif) Configurez l'intervalle de mise à jour entre les requêtes DNS.

interval maximum *days hours minutes seconds*

Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres *days* (jours) (0-364), *hours* (heures), *minutes* et *seconds* (secondes).

Exemple :

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

f) Associez cette méthode à une interface. Consultez Étape 3, à la page 873.

g) La méthode de type Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS. Voir l'étape Étape 4, à la page 875.

Étape 3 Configurez les paramètres d'interface pour DDNS, y compris la définition de la méthode de mise à jour, les paramètres du client DHCP et le nom d'hôte pour cette interface.

a) Entrez en mode de configuration d'interface.

interface *ID*

Exemple :

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)#
```

b) Attribuez une méthode de mise à jour.

ddns update *name*

Méthode DDNS standard : vous n'avez pas besoin d'attribuer de méthode si vous souhaitez que le serveur DHCP effectue toutes les mises à jour. Cette commande est requise pour la méthode de mise à jour Web.

Exemple :

```
ciscoasa(config-if)# ddns update ddns1
```

c) Attribuez un nom d'hôte à cette interface.

ddns update hostname *hostname*

Si vous ne définissez pas de nom d'hôte, le nom d'hôte du périphérique est utilisé. Si vous ne spécifiez pas de FQDN, le nom de domaine système ou le domaine par défaut du groupe de serveurs DNS est ajouté (pour les adresses IP statiques ou PPPoE) ou le nom de domaine du serveur DHCP est ajouté (pour les adresses IP DHCP).

Exemple :

```
ciscoasa(config-if)# ddns update hostname asa1.example.com
```

d) Méthode DDNS standard : déterminez les enregistrements que vous souhaitez que le serveur DHCP mette à jour.

dhcp client update dns [**server** {**both** | **none**}]

L'ASA envoie les requêtes des clients DHCP au serveur DHCP. Notez que le serveur DHCP doit également être configuré pour prendre en charge DDNS. Le serveur peut être configuré pour répondre aux demandes du client ou il peut remplacer les commandes du client (auquel cas, il répondra au client pour que le client n'essaye pas également d'effectuer les mises à jour effectuées par le serveur). Même si le client ne demande pas de mises à jour DDNS, le serveur DHCP peut être configuré pour envoyer quand même des mises à jour.

Pour les adresses IP statiques ou PPPoE, ces paramètres sont ignorés.

Remarque
Vous pouvez également définir ces valeurs globalement pour toutes les interfaces à l'aide de la commande **dhcp-client update dns**. Les paramètres par interface prévalent sur les paramètres globaux.

- Par défaut (sans mot clé) : demande au serveur DHCP d'effectuer la mise à jour des RR PTR. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les enregistrements **ddns** A activés.
- **server both** : demande au serveur DHCP d'effectuer les mises à jour des enregistrements A et RR PTR. Ce paramètre ne nécessite pas l'association d'une méthode de mise à jour DDNS à l'interface.
- **server none** : demande au serveur DHCP de ne pas effectuer de mises à jour. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les enregistrements **ddns both** A et PTR activés.

Exemple :

```
ciscoasa(config-if)# ddns client update dns
```

Étape 4 La méthode Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS. Consultez Configurer les points de confiance, à la page 898.

Exemple :

```
crypto ca trustpoint DDNS_Trustpoint
  enrollment terminal
crypto ca authenticate DDNS_Trustpoint nointeractive
   MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
   MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
   [...]
   quit
```

Méthode DDNS standard pour une adresse IP statique

L'exemple suivant montre comment configurer la méthode DDNS standard pour une utilisation avec une adresse IP statique. Notez que vous ne configurez pas les paramètres du client DHCP pour ce scénario.

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
 ddns both
interface gigabitethernet1/1
 ip address 209.165.200.225
! Associate the method with the interface:
 ddns update ddns-2
 ddns update hostname asa1.example.com
```

Exemple : méthode DDNS standard; mises à jour RR A de l'ASA et mises à jour RR PTR du serveur DHCP

L'exemple suivant configure l'ASA pour mettre à jour le RR A et le serveur DHCP pour mettre à jour le RR PTR.

```
! Define the DDNS method to update the A RR:
ddns update method ddns-1
 ddns
interface gigabitethernet1/1
  ip address dhcp
! Associate the method with the interface:
  ddns update ddns-1
  ddns update hostname asa
! Set the client to update the A RR, and the server to update the PTR RR:
  dhcp client update dns
```

Exemple : méthode DDNS standard; aucune mise à jour des RR du serveur DHCP

L'exemple suivant configure l'ASA pour mettre à jour le RR A et PTR, tout en demandant au serveur DHCP de mettre à jour les RR.

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
  ddns both
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
```

```
  ddns update ddns-2
  ddns update hostname asa1.example.com
! Set the client to update both RRs, and the server to update none:
  dhcp client update dns server none
```

Exemple : méthode DDNS standard; le serveur DHCP met à jour tous les RR

L'exemple suivant configure le client DHCP pour demander au serveur DHCP de mettre à jour les RR A et PTR. Étant donné que le serveur effectue toutes les mises à jour, il n'est pas nécessaire d'associer une méthode de mise à jour à l'interface.

```
interface gigabitethernet1/1
  ip address dhcp
  ddns update hostname asa
! Configure the DHCP server to update both RRs:
  dhcp client update dns server both
```

Exemple : type Web

L'exemple suivant configure la méthode du type Web.

```
! Define the web type method:
ddns update method web-1
  web update-url https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

Supervision des services DHCP et DDNS

Cette section comprend les procédures pour superviser les services DHCP et DDNS.

Supervision des services DHCP

- **show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

  Cette commande affiche les statistiques, l'état et la liaison du client du serveur DHCP actuel.

- **show dhcprelay** {**state** | **statistics**}

  Cette commande affiche l'état et les statistiques du relais DHCP.

- **show ipv6 dhcprelay binding**

  Cette commande affiche les entrées de liaison de relais qui ont été créées par l'agent de relais.

- **show ipv6 dhcprelay statistics**

  Cette commande affiche les statistiques de l'agent de relais DHCP pour IPv6.

- **show ipv6 dhcp server statistics**

  Cette commande affiche les statistiques du serveur sans état DHCPv6. L'exemple suivant montre les renseignements fournis par cette commande :

```
ciscoasa(config)# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                  10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp pool** [*pool_name*]
- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  La commande **show ipv6 dhcp interface** affiche les renseignements DHCPv6 pour toutes les interfaces. Si l'interface est configurée pour la configuration du serveur sans état DHCPv6 (voir Configurer le serveur sans état DHCPv6, à la page 865), cette commande répertorie l'ensemble DHCPv6 utilisé par le serveur. Si l'interface a une configuration de client d'adresse DHCPv6 ou de client de délégation de préfixe, cette commande affiche l'état de chaque client et les valeurs reçues du serveur. Pour une interface en particulier, vous pouvez afficher les statistiques des messages pour le serveur ou le client DHCP. Les exemples suivants montrent les renseignements fournis par cette commande :

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD
```

```
Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                 preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

La commande **show ipv6 dhcp ha statistics** affiche les statistiques de transaction entre les unités de basculement, y compris le nombre de fois où les renseignements DUID ont été synchronisés entre les unités. Les exemples suivants montrent les renseignements fournis par cette commande.

Sur une unité active :

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

Sur une unité de secours :

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

Dépannage du relais DHCP sur VTI

Si le client DHCP ne parvient pas à obtenir une adresse IP :

- Vérifiez la configuration de l'interface de tunnel/VTI dans les deux sites ASA.
- Vérifiez les paquets transférés entre les sites à l'aide de la commande **show crypto ipsec sa** :

  Exemple

```
ciscoasa(config)# show crypto ipsec sa
interface: outside
Crypto map tag: cmap, seq num: 10, local addr: 192.168.2.111
access-list CSM_IPSEC_ACL_0 extended permit ip any4 any4
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.2.110
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
```

Activer les commandes de débogage

L'activation des débogages de relais DHCP vous aide à savoir si les paquets DISOVER/REQUEST ont été transférés vers le serveur de relais DHCP :

- **debug dhcprelay event 255**
- **debug dhcprelay packet 255**
- **debug dhcprelay error 255**

Exemple

```
ciscoasa(config)# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
DHCP: Received a BOOTREQUEST from interface 2 (size = 548)
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPRA: setting giaddr to 192.168.1.111. dhcpd_forward_request: request from xxxx.xxxx.xxxx
forwarded to 192.168.3.112.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on vti interface
DHCP: Received a BOOTREPLY from relay interface 5 (size = 300, xid = xxxxxxxxx) at 04:40:52
UTC Tue Sep 10 2019
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPD/RA: creating ARP entry (192.168.1.88, xxxx.xxxx.xxxx).
DHCPRA: Adding rule to allow client to respond using offered address 192.168.1.95
DHCPRA: forwarding reply to client xxxx.xxxx.xxxx.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
```

Supervision de l'état DDNS

Consultez la commande suivante pour superviser l'état du DDNS.

- **show ddns update** {**interface** *if_name* | **method** [*name*]}

  Cette commande affiche l'état de la mise à jour du DDNS.

  L'exemple suivant montre les détails de la méthode de mise à jour du DDNS :

```
ciscoasa# show ddns update method ddns1

Dynamic DNS Update Method: ddns1
  IETF standardized Dynamic DNS 'A' record update
```

  L'exemple suivant montre les détails de la méthode de mise à jour Web :

```
ciscoasa# show ddns update method web1

Dynamic DNS Update Method: web1
 Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

  L'exemple suivant montre les renseignements relatifs à l'interface DDNS :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available
```

  L'exemple suivant montre une mise à jour de type Web réussie :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : asa1.example.com
```

```
IP addresses(s): 10.10.32.45,2001:DB8::1
```

L'exemple suivant montre une défaillance de type Web :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

L'exemple suivant montre que le serveur DNS a renvoyé une erreur pour la mise à jour du type Web :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

L'exemple suivant montre qu'une mise à jour Web n'a pas encore été tentée en raison de l'adresse IP non configurée ou de l'échec de la requête DHCP, par exemple :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

Historique des services DHCP et DDNS

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de DDNS pour la méthode de mise à jour Web	9.15(1)	Vous pouvez maintenant configurer une interface pour utiliser DDNS avec la méthode de mise à jour Web. Commandes nouvelles ou modifiées : **show ddns update interface**, **show ddns update method**, **web update-url**, **web update-type**
Prise en charge du serveur de relais DHCP sur les VTI	9.14(1)	Vous pouvez maintenant activer le relais DHCP sur les VTI. Commandes nouvelles ou modifiées : **dhcprelay server** .

Nom de la caractéristique	Versions de plateforme	Description
Réservation DHCP	9.13(1)	L'ASA prend en charge la réservation DHCP. Le serveur DHCP attribue une adresse IP statique à partir de l'ensemble d'adresses à un client DHCP en fonction de l'adresse MAC du client. Commandes nouvelles ou modifiées : **dhcpd reserve-address** .
DHCP IPv6	9.6(2)	L'ASA prend désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 : • Client d'adresse DHCPv6 : l'ASA obtient une adresse globale IPv6 et une route par défaut facultative du serveur DHCPv6. • Client de délégation de préfixe DHCPv6 : l'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. • Annonce de routeur BGP pour les préfixes délégués • Serveur sans état DHCPv6 : l'ASA fournit d'autres renseignements tels que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresses aux clients. Nous avons ajouté ou modifié les commandes suivantes : **clear ipv6 dhcp statistics, domain-name, dns-server, import, ipv6 address, ipv6 address dhcp, ipv6 dhcp client pd, ipv6 dhcp client pd hint, ipv6 dhcp pool, ipv6 dhcp server, network, nis address, nis domain-name, nisp address, nisp domain-name, show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix, sip address, sip domain-name, sntp address**
Supervision DHCPv6	9.4(1)	Vous pouvez maintenant superviser les statistiques DHCP pour IPv6 et les liaisons DHCP pour IPv6.
Le serveur de relais DHCP valide l'identifiant du serveur DHCP pour les réponses	9.2(4)/9.3(3)	Si le serveur de relais DHCP ASA reçoit une réponse d'un serveur DHCP incorrect, il vérifie désormais que la réponse provient du bon serveur avant de donner suite à la réponse. Nous n'avons pas introduit ni modifié de commandes. Nous n'avons pas modifié d'écrans ASDM. Nous n'avons pas introduit ni modifié de commandes.
Fonction de liaison DHCP	9.1(4)	Pendant la phase de liaison DHCP, le client tente maintenant de se rétablir d'autres serveurs DHCP dans la liste des groupes du tunnel. Avant cette version, le client ne se reconnectait pas à un autre serveur lorsque le renouvellement du bail DHCP échouait. Nous n'avons pas introduit ni modifié de commandes.

Nom de la caractéristique	Versions de plateforme	Description
Interfaces de confiance DHCP	9.1(2)	Vous pouvez désormais configurer des interfaces en tant qu'interfaces de confiance pour conserver l'option 82 de DHCP. L'option 82 DHCP est utilisée par les commutateurs et les routeurs en aval pour la surveillance DHCP et la protection source IP. Normalement, si l'agent de relais DHCP ASA reçoit un paquet DHCP avec l'option 82 déjà définie, mais que le champ giaddr (qui spécifie l'adresse de l'agent de relais DHCP définie par ce dernier avant de transmettre le paquet au serveur) est réglé sur 0, l'ASA supprimera ce paquet par défaut. Vous pouvez désormais conserver l'option 82 et transférer le paquet en identifiant une interface comme interface de confiance. Nous avons introduit ou modifié les commandes suivantes : **dhcprelay information trusted**, **dhcprelay information trust-all**, **show running-config dhcprelay**.
Serveurs de relais DHCP par interface (IPv4 uniquement)	9.1(2)	Vous pouvez désormais configurer des serveurs de relais DHCP par interface, de sorte que les demandes qui entrent dans une interface donnée ne sont relayées que vers les serveurs spécifiés pour cette interface. IPv6 n'est pas pris en charge pour le relais DHCP par interface. Nous avons introduit ou modifié les commandes suivantes : **dhcprelay server** (mode de configuration d'interface), **clear configure dhcprelay**, **show running-config dhcprelay**.
Relais DHCP pour IPv6 (DHCPv6)	9.0(1)	La prise en charge des relais DHCP pour IPv6 a été ajoutée. Nous avons introduit les commandes suivantes : **ipv6 dhcprelay server**, **ipv6 dhcprelay enable**, **ipv6 dhcprelay timeout**, **clear config ipv6 dhcprelay**, **ipv6 nd managed-config-flag**, **ipv6 nd other-config-flag**, **debug ipv6 dhcp**, **debug ipv6 dhcprelay**, **show ipv6 dhcprelay binding**, **clear ipv6 dhcprelay binding**, **show ipv6 dhcprelay statistics** et **clear ipv6 dhcprelay statistics**.
Système de nom de domaine dynamique (DDNS)	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les commandes suivantes : **ddns**, **ddns update**, **dhcp client update dns**, **dhcpd update dns**, **show running-config ddns** et **show running-config dns server-group**.
DHCP (protocole de configuration dynamique des hôtes)	7.0(1)	L'ASA peut fournir un serveur DHCP ou des services de relais DHCP aux clients DHCP connectés aux interfaces ASA. Nous avons introduit les commandes suivantes : **dhcp client update dns**, **dhcpd address**, **dhcpd domain**, **dhcpd enable**, **dhcpd lease**, **dhcpd option**, **dhcpd ping timeout**, **dhcpd update dns**, **dhcpd wins**, **dhcp-network-scope**, **dhcprelay enable**, **dhcprelay server**, **dhcprelay setroute**, **dhcp-server**. **show running-config dhcpd** et **show running-config dhcprelay**.



CHAPITRE 25

Certificats numériques

Ce chapitre décrit comment configurer les certificats numériques.

- À propos des certificats numériques, à la page 885
- Lignes directrices pour les certificats numériques, à la page 893
- Configurer les certificats numériques, à la page 896
- Comment configurer des types de certificats spécifiques, à la page 917
- Définir une alerte d'expiration de certificat (pour les certificats d'identité ou CA), à la page 919
- Supervision des certificats numériques, à la page 920
- Historique de gestion des certificats, à la page 922

À propos des certificats numériques

Les certificats numériques fournissent une identification numérique aux fins d'authentification. Un certificat numérique contient des renseignements permettant d'identifier un appareil ou un utilisateur, tels que le nom, le numéro de série, l'entreprise, le service ou l'adresse IP. Les autorités de certification sont chargées de gérer les demandes de certificat et d'émettre des certificats numériques. Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur.

Un certificat numérique inclut également une copie de la clé publique de l'utilisateur ou du périphérique. Une autorité de certification peut être un tiers de confiance, comme VeriSign, ou une autorité de certification privée (interne) que vous établissez au sein de votre organisation. Les autorités de certification émettent des certificats numériques dans le contexte d'une PKI, qui utilise le chiffrement par clé publique ou par clé privée pour assurer la sécurité.

Pour l'authentification à l'aide de certificats numériques, au moins un certificat d'identité et son certificat CA d'émission doivent exister sur un ASA. Cette configuration autorise plusieurs identités, racines et hiérarchies de certificat. L'ASA évalue les certificats tiers par rapport aux CRL, également appelées listes de révocation d'autorité, depuis le certificat d'identité jusqu'à la chaîne des autorités de certification subordonnées.

Voici une description de plusieurs types de certificats numériques disponibles :

- Un certificat d'autorité de certification est utilisé pour signer les autres certificats. Il est autosigné et appelé certificat racine. Un certificat émis par un autre certificat CA s'appelle un certificat subordonné.
- Les autorités de certification délivrent également des certificats d'identité, qui sont des certificats pour des systèmes ou des hôtes spécifiques.

- Les certificats de signataire de code sont des certificats spéciaux utilisés pour créer des signatures numériques pour signer le code, le code signé révélant lui-même l'origine du certificat.

Dans une hiérarchie avec une racine et deux certificats CA intermédiaires, une validation de CRL pour l'accès à distance échoue sur la tête de réseau exécutant la version 9.13 ou une version ultérieure lorsque le certificat d'ID est signé par une CA intermédiaire, mais que la CRL est signée par une autre CA intermédiaire. La défaillance se produit même si la tête de réseau fait confiance aux deux intermédiaires lorsque ceux-ci sont signés par la même racine.

Par conséquent, chaque signataire doit conserver sa propre CRL. Chaque signataire précisera ensuite l'emplacement de la CRL dans la liste d'URL de chaque certificat qu'il signe. Sinon, vous pouvez configurer un remplacement d'URL dans le point de confiance de chaque signataire pointant vers le bon emplacement de CRL.

La CA locale intègre une fonctionnalité d'autorité de certificat indépendante sur l'ASA, déploie les certificats et assure une vérification sécurisée de la révocation des certificats émis. La CA locale fournit une autorité interne sécurisée et configurable pour l'authentification des certificats avec inscription des utilisateurs via une page de connexion au site Web.

Remarque Les certificats CA et les certificats d'identité s'appliquent à la fois aux connexions VPN de site à site et aux connexions VPN d'accès à distance. Les procédures dans ce document font référence à l'utilisation du VPN d'accès à distance dans l'interface graphique utilisateur du gestionnaire ASDM.

Astuces Pour un exemple de scénario comprenant la configuration des certificats et l'équilibrage de charges, consultez l'URL suivante : https://supportforums.cisco.com/docs/DOC-5964.

Cryptographie à clé publique

Les signatures numériques, activées par le chiffrement à clé publique, fournissent un moyen d'authentifier les appareils et les utilisateurs. Dans le chiffrement à clé publique, comme le système de chiffrement RSA, chaque utilisateur dispose d'une paire de clés contenant une clé publique et une clé privée. Les clés agissent comme des compléments, et tout ce qui est chiffré avec l'une des clés peut être déchiffré avec l'autre.

En termes simples, une signature se forme lorsque les données sont chiffrées avec une clé privée. La signature est jointe aux données et envoyée au récepteur. Le récepteur applique la clé publique de l'expéditeur aux données. Si la signature envoyée avec les données correspond au résultat de l'application de la clé publique aux données, la validité du message est établie.

Ce processus repose sur le récepteur ayant une copie de la clé publique de l'expéditeur et sur un degré élevé de confiance que cette clé appartient à l'expéditeur, et non à une personne se faisant passer pour l'expéditeur.

L'obtention de la clé publique d'un expéditeur est normalement gérée en externe ou par le biais d'une opération effectuée lors de l'installation. Par exemple, la plupart des navigateurs Web sont configurés avec les certificats racine de plusieurs autorités de certification par défaut. Pour le VPN, le protocole IKE, un composant IPsec, peut utiliser des signatures numériques pour authentifier les périphériques homologues avant de configurer des associations de sécurité.

Évolutivité des certificats

Sans certificats numériques, vous devez configurer manuellement chaque homologue IPsec pour chaque homologue avec lequel il communique; par conséquent, chaque nouvel homologue que vous ajoutez à un réseau nécessite une modification de configuration sur chaque homologue avec lequel il doit communiquer de manière sécurisée.

Lorsque vous utilisez des certificats numériques, chaque homologue est inscrit auprès d'une CA. Lorsque deux homologues tentent de communiquer, ils échangent des certificats et signent numériquement les données pour s'authentifier. Lorsqu'un nouvel homologue est ajouté au réseau, vous inscrivez cet homologue auprès d'une CA et aucun des autres homologues ne nécessite de modification. Lorsque le nouvel homologue tente une connexion IPsec, les certificats sont automatiquement échangés et l'homologue peut être authentifié.

Avec une CA, un homologue s'authentifie auprès de l'homologue distant en lui envoyant un certificat et en effectuant une cryptographie à clé publique. Chaque homologue envoie son certificat unique, qui a été émis par la CA. Ce processus fonctionne, car chaque certificat encapsule la clé publique de l'homologue associé, chaque certificat est authentifié par la CA et tous les homologues participants reconnaissent la CA comme une autorité d'authentification. Le processus s'appelle IKE avec une signature RSA.

L'homologue peut continuer à envoyer son certificat pour plusieurs sessions IPsec et à plusieurs homologues IPsec jusqu'à l'expiration du certificat. Lorsque son certificat expire, l'administrateur homologue doit en obtenir un nouveau auprès de la CA.

Les CA peuvent également révoquer les certificats d'homologues qui ne participent plus à IPsec. Les certificats révoqués ne sont pas reconnus comme valides par les autres homologues. Les certificats révoqués sont répertoriés dans une CRL, que chaque homologue peut vérifier avant d'accepter un certificat d'un autre homologue.

Certaines CA disposent d'une autorité d'enregistrement dans le cadre de leur mise en œuvre. Une autorité d'enregistrement est un serveur qui agit en tant que mandataire pour la CA, de sorte que les fonctions CA puissent continuer à fonctionner lorsque la CA n'est pas disponible.

Paires de clés

Les paires de clés sont des clés d'algorithme de signature numérique à courbe elliptique (ECDSA), qui ont les caractéristiques suivantes :

- Les clés RSA peuvent être utilisées pour SSH ou SSL.
- L'inscription SCEP prend en charge la certification des clés RSA.
- La taille de clé RSA maximum est de 4 096 et la valeur par défaut est de 2 048.
- La longueur maximum de la clé ECDSA est de 521, et la valeur par défaut est de 384.
- Vous pouvez générer une paire de clés RSA à usage général, utilisée à la fois pour la signature et le chiffrement, ou vous pouvez générer des paires de clés RSA distinctes pour chaque objectif. Des clés de signature et de chiffrement distinctes aident à réduire l'exposition des clés, car SSL utilise une clé pour le chiffrement, mais pas pour la signature. Cependant, IKE utilise une clé pour la signature, mais pas pour le chiffrement. En utilisant des clés distinctes pour chacune, l'exposition des clés est réduite au minimum.

Point de confiance

Les points de confiance vous permettent de gérer et de suivre les autorités de certification et les certificats. Un point de confiance est la représentation d'une autorité de certification ou d'une paire d'identités. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres de configuration spécifiques à l'autorité de certification et une association avec un certificat d'identité inscrit.

Après avoir défini un point de confiance, vous pouvez le référencer par son nom dans les commandes nécessitant de spécifier une CA. Vous pouvez configurer de nombreux points de confiance.



Remarque Si l'ASA a plusieurs points de confiance qui partagent la même CA, un seul de ces points de confiance partageant la CA peut être utilisé pour valider les certificats d'utilisateur. Pour contrôler le partage du point de confiance qu'une CA utilise pour la validation des certificats d'utilisateur émis par cette CA, utilisez la commande **support-user-cert-validation**.

Pour l'inscription automatique, un point de confiance doit être configuré avec une URL d'inscription, et la CA que représente le point de confiance doit être disponible sur le réseau et doit prendre en charge SCEP.

Vous pouvez exporter et importer la paire de clés et les certificats émis associés à un point de confiance au format PKCS12. Ce format est utile pour dupliquer manuellement une configuration de point de confiance sur un autre ASA.

Inscription de certificat

L'ASA a besoin d'un certificat CA pour chaque point de confiance et d'un ou deux certificats pour lui-même, selon la configuration des clés utilisées par le point de confiance. Si le point de confiance utilise des clés RSA distinctes pour la signature et le chiffrement, l'ASA a besoin de deux certificats, un pour chaque fonction. Dans les autres configurations de clés, un seul certificat est nécessaire.

L'ASA prend en charge l'inscription automatique avec SCEP et l'inscription manuelle, ce qui vous permet de coller un certificat codé en base 64 directement dans le terminal. Pour les VPN de site à site, vous devez inscrire chaque ASA. Pour les VPN d'accès à distance, vous devez inscrire chaque ASA et chaque client VPN d'accès à distance.

Serveur mandataire pour les demandes SCEP

L'ASA peut servir de mandataire pour les demandes SCEP entre Secure Client (services client sécurisés) et une CA tierce. La CA ne doit être accessible à l'ASA que si celui-ci agit en tant que mandataire. Pour que l'ASA fournisse ce service, l'utilisateur doit s'authentifier à l'aide de l'une des méthodes prises en charge par AAA avant que l'ASA envoie une demande d'inscription. Vous pouvez également utiliser l'analyse de l'hôte et des politiques d'accès dynamique pour appliquer des règles d'admissibilité à l'inscription.

L'ASA prend en charge cette fonctionnalité uniquement avec une session VPN Secure Client (services client sécurisés) SSL ou IKEv2. Il prend en charge toutes les autorités de certification conformes à SCEP, y compris Cisco IOS CS, Windows Server 2003 CA et Windows Server 2008 CA

L'accès sans client (par navigateur) ne prend pas en charge le mandataire SCEP, bien que WebLaunch (Secure Client (services client sécurisés) initié sans client) le prenne en charge.

L'ASA ne prend pas en charge l'interrogation des certificats.

L'ASA prend en charge l'équilibrage de charges pour cette fonctionnalité.

Vérification de la révocation

Lorsqu'un certificat est émis, il est valide pour une période fixe. Parfois, une CA révoque un certificat avant l'expiration de cette période; par exemple, en raison de problèmes de sécurité ou d'un changement de nom ou d'association. Les CA publient périodiquement une liste signée des certificats révoqués. L'activation de la vérification de la révocation force l'ASA à vérifier que la CA n'a pas révoqué un certificat chaque fois qu'il l'utilise pour l'authentification.

Lorsque vous activez la vérification de la révocation, l'ASA vérifie l'état de révocation du certificat pendant le processus de validation du certificat PKI, qui peut utiliser la vérification des CRL, OCSP ou les deux. Le protocole OCSP est uniquement utilisé lorsque la première méthode renvoie une erreur (par exemple, indiquant que le serveur n'est pas disponible).

Lors de la vérification des CRL, l'ASA récupère, analyse et met en mémoire cache les CRL, qui fournissent une liste complète des certificats révoqués (et non révoqués) avec leurs numéros de série. L'ASA évalue les certificats en fonction des CRL, également appelées listes de révocation d'autorité, à partir du certificat d'identité jusqu'à la chaîne des autorités de certification subordonnées.

Le protocole OCSP offre une méthode plus évolutive de vérification de l'état de révocation dans la mesure où il localise l'état du certificat auprès d'une autorité de validation, à laquelle il demande l'état d'un certificat spécifique.

Serveurs CA pris en charge

L'ASA prend en charge les serveurs CA suivants :

CS Cisco IOS, CA local ASA et les prestataires CA tiers conformes à X.509, y compris, sans s'y limiter :

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

Les CRL fournissent à l'ASA un moyen de déterminer si un certificat qui se trouve dans sa plage de temps valide a été révoqué par la CA émettrice. La configuration des CRL fait partie de la configuration d'un point de confiance.

Vous pouvez configurer l'ASA pour rendre les vérifications de CRL obligatoires lors de l'authentification d'un certificat à l'aide de la commande **revocation-check crl**. Vous pouvez également rendre la vérification

de la CRL facultative en utilisant la commande **revocation-check crl none**, qui permet de réussir l'authentification par certificat lorsque la CA n'est pas disponible pour fournir des données CRL mises à jour.

Remarque La commande **revocation-check crl none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

L'ASA peut récupérer les CRL des autorités de certification à l'aide de HTTP, SCEP ou LDAP. Les CRL extraites pour chaque point de confiance sont mises en cache pour une durée configurable pour chaque point de confiance.

Remarque Même si le serveur CRL répond par l'indicateur HTTP « Connection: Keep-alive » (Connexion : Keepalive) pour indiquer une connexion persistante, l'ASA ne demande pas la prise en charge de la connexion persistante. Modifiez les paramètres sur le serveur CRL pour répondre par « Connection: Close » (Connexion : Fermer) lorsque la liste est envoyée.

Lorsque l'ASA a mis en cache une CRL plus longtemps que la configuration de la mise en cache des CRL, l'ASA considère la CRL comme trop ancienne pour être fiable ou « obsolète ». L'ASA tente de récupérer une version plus récente de la CRL la prochaine fois qu'une authentification par certificat nécessite une vérification de la CRL obsolète.

Vous pourriez recevoir un échec de *vérification de la révocation* pour une connexion ou un certificat utilisateur si vous dépassez la limite de taille de 16 Mo pour la CRL.

L'ASA met les CRL en cache pendant une durée déterminée par les deux facteurs suivants :

- Le nombre de minutes spécifié avec la commande **cache-time**. La valeur par défaut est de 60 minutes.
- Le champ NextUpdate dans les CRL extraites, qui peut être absent des CRL. Vous contrôlez si l'ASA requiert et utilise le champ NextUpdate avec la commande **enforcenextupdate**.

L'ASA utilise ces deux facteurs de la manière suivante :

- Si le champ NextUpdate n'est pas obligatoire, l'ASA marque les CRL comme obsolètes après la durée définie par la commande **cache-time**.
- Si le champ NextUpdate est obligatoire, l'ASA marque les CRL comme obsolètes à la première des deux fois spécifiées par la commande **cache-time** et le champ NextUpdate. Par exemple, si la commande **cache-time** est définie à 100 minutes et que le champ NextUpdate indique que la prochaine mise à jour est à 70 minutes, l'ASA marque les CRL comme obsolètes en 70 minutes.

Si l'ASA a une mémoire insuffisante pour stocker toutes les CRL mises en cache pour un point de confiance donné, il supprime la CRL la moins récemment utilisée pour faire de la place pour une CRL nouvellement récupérée. Les grandes CRL nécessitent un surdébit de calcul important pour les analyser. Par conséquent, pour de meilleures performances, utilisez de nombreuses CRL de plus petite taille plutôt que quelques grandes CRL, ou de préférence, utilisez OCSP.

Consultez les tailles de cache suivantes :

- Mode de contexte unique : 128 Mo
- Mode de contexte multiple : 16 Mo par contexte

OCSP

L'OCSP fournit à l'ASA un moyen de déterminer si un certificat qui se trouve dans sa plage de temps valide a été révoqué par la CA émettrice. La configuration de l'OCSP fait partie de la configuration du point de confiance.

L'OCSP localise l'état du certificat sur une autorité de validation (un serveur OCSP, également appelé *répondeur*) que l'ASA interroge pour connaître l'état d'un certificat en particulier. Cette méthode offre une meilleure évolutivité et un état de révocation plus à jour que la vérification des CRL, et aide les entreprises avec de grandes installations PKI à déployer et à étendre des réseaux sécurisés.



Remarque L'ASA autorise un décalage de cinq secondes pour les réponses OCSP.

Vous pouvez configurer l'ASA pour rendre les vérifications OCSP obligatoires lors de l'authentification d'un certificat à l'aide de la commande **revocation-check ocsp**. Vous pouvez également rendre la vérification OCSP facultative en utilisant la commande **revocation-check ocsp none**, qui permet de réussir l'authentification par certificat lorsque l'autorité de validation n'est pas disponible pour fournir des données OCSP mises à jour.



Remarque La commande **revocation-check ocsp none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

L'OCSP fournit trois façons de définir l'URL du serveur OCSP. L'ASA utilise ces serveurs dans l'ordre suivant :

1. L'URL OCSP définie dans une règle de remplacement de certificat de correspondance à l'aide de la commande **match certificate**).
2. L'URL OCSP configurée à l'aide de la commande **ocsp url**.
3. Le champ AIA du certificat client.



Remarque Pour configurer un point de confiance pour valider un certificat de répondeur OCSP autosigné, vous devez importer le certificat de répondeur autosigné dans son propre point de confiance en tant que certificat CA de confiance. Ensuite, vous devez configurer la commande **match certificate** dans le point de confiance de validation du certificat client pour utiliser le point de confiance qui comprend le certificat de répondeur OCSP autosigné pour valider le certificat de répondeur. Utilisez la même procédure pour configurer la validation des certificats de répondeur externes au chemin de validation du certificat client.

Le certificat du serveur OCSP (répondeur) signe généralement la réponse OCSP. Après avoir reçu la réponse, l'ASA tente de vérifier le certificat du répondeur. La CA définit normalement la durée de vie du certificat de répondeur OCSP sur une période relativement courte pour réduire au minimum les risques de compromission. La CA comprend généralement une extension ocsp-no-check dans le certificat du répondeur, qui indique que ce certificat n'a pas besoin de vérification de l'état de révocation. Cependant, si cette extension est absente, l'ASA tente de vérifier l'état de révocation en utilisant la même méthode que spécifiée dans le point de confiance. Si le certificat du répondeur n'est pas vérifiable, les vérifications de révocation échouent. Pour éviter cette possibilité, utilisez la commande **revocation-check none** pour configurer le point de confiance de validation du certificat du répondeur et utilisez la commande **revocation-check ocsp** pour configurer le certificat client.

Certificats et coordonnées de connexion de l'utilisateur

La section suivante décrit les différentes méthodes d'utilisation des certificats et des coordonnées de connexion de l'utilisateur (nom d'utilisateur et mot de passe) pour l'authentification et l'autorisation. Ces méthodes s'appliquent à IPsec, Secure Client (services client sécurisés) et au SSL VPN sans client.

Dans tous les cas, l'autorisation LDAP n'utilise pas le mot de passe comme identifiant. L'autorisation RADIUS utilise un mot de passe commun pour tous les utilisateurs ou le nom d'utilisateur comme mot de passe.

Informations d'authentification de l'utilisateur

La méthode par défaut pour l'authentification et l'autorisation utilise les coordonnées de connexion de l'utilisateur.

- Authentification
  - Activé par le paramètre du groupe de serveurs d'authentification dans le groupe de tunnels (également appelé profil de connexion ASDM)
  - Utilise le nom d'utilisateur et le mot de passe comme identifiant
- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation dans le groupe de tunnels (également appelé profil de connexion ASDM)
  - Utilise le nom d'utilisateur comme identifiant

Certificats

Si des certificats numériques d'utilisateur sont configurés, l'ASA valide d'abord le certificat. Cependant, il n'utilise aucun des DN des certificats comme nom d'utilisateur pour l'authentification.

Si l'authentification et l'autorisation sont toutes deux activées, l'ASA utilise les coordonnées de connexion de l'utilisateur pour l'authentification et l'autorisation de l'utilisateur.

- Authentification
  - Activé par le paramètre du groupe de serveurs d'authentification
  - Utilise le nom d'utilisateur et le mot de passe comme identifiant
- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation
  - Utilise le nom d'utilisateur comme identifiant

Si l'authentification est désactivée et que l'autorisation est activée, l'ASA utilise le champ DN principal pour l'autorisation.

- Authentification
  - DÉSACTIVÉ (défini sur Aucun) par le paramètre du groupe de serveurs d'authentification
  - Aucun identifiant utilisé

- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation
  - Utilise la valeur du nom d'utilisateur du champ DN principal du certificat comme identifiant



Remarque Si le champ de DN principal n'est pas présent dans le certificat, l'ASA utilise la valeur du champ DN secondaire comme nom d'utilisateur pour la demande d'autorisation.

Prenons par exemple un certificat d'utilisateur qui comprend les champs et les valeurs de DN du sujet suivants :

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

Si le DN principal = EA (adresse courriel) et le DN secondaire = CN (nom commun), le nom d'utilisateur utilisé dans la demande d'autorisation serait anyuser@example.com.

Lignes directrices pour les certificats numériques

Cette section comprend des lignes directrices et des limites que vous devez vérifier avant de configurer les certificats numériques.

Directives relatives au mode contextuel

- Pris en charge en mode de contexte unique seulement pour les autorités de certification tierces.

Directives en matière de basculement

- Ne prend pas en charge la réplication des sessions dans le basculement dynamique.
- Ne prend pas en charge le basculement pour les autorités de certification locales.
- Les certificats sont automatiquement copiés sur l'unité de secours si vous configurez le basculement dynamique. Si vous constatez qu'un certificat est manquant, utilisez la commande **write standby** sur l'unité active.

Directives IPv6

Ne prend pas en charge IPv6.

Certificats de CA locale

- Assurez-vous que l'ASA est configuré correctement pour prendre en charge les certificats. Un ASA mal configuré peut entraîner l'échec de l'inscription ou demander un certificat contenant des renseignements inexacts.
- Assurez-vous que le nom d'hôte et le nom de domaine de l'ASA sont configurés correctement. Pour afficher le nom d'hôte et le nom de domaine actuellement configurés, saisissez la commande **show running-config**.

- Assurez-vous que l'horloge ASA est réglée avec précision avant de configurer la CA. Les certificats ont une date et une heure de validité et d'expiration. Lorsque l'ASA s'inscrit auprès d'une CA et obtient un certificat, l'ASA vérifie que l'heure actuelle se situe dans la plage de validité du certificat. Si ce n'est pas le cas, l'inscription échoue.
- Trois jours avant l'expiration du certificat de CA locale, un certificat de renouvellement de remplacement est généré et un message de journal système informe l'administrateur qu'il est temps de procéder au renouvellement du certificat de CA locale. Le nouveau certificat de CA locale doit être importé sur tous les périphériques nécessaires avant l'expiration du certificat actuel. Si l'administrateur ne répond pas en installant le certificat de renouvellement comme nouveau certificat de CA locale, les validations peuvent échouer.
- Le certificat de CA locale est renouvelé automatiquement après son expiration en utilisant la même paire de clés. Le certificat de renouvellement peut être exporté au format base 64.

  L'exemple suivant montre un certificat de CA locale codé en base 64 :

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

Prise en charge du mandataire SCEP

- Assurez-vous que l'ASA et les nœuds de service de politique Cisco ISE sont synchronisés à l'aide du même serveur NTP.
- Secure Client (services client sécurisés) 3.0 ou une version ultérieure doit être en cours d'exécution sur le terminal.
- La méthode d'authentification, configurée dans le profil de connexion pour votre stratégie de groupe, doit être définie pour utiliser à la fois AAA et l'authentification par certificat.
- Un port SSL doit être ouvert pour les connexions VPN IKEv2.
- La CA doit être en mode d'octroi automatique.

Directives supplémentaires

- Le type de certificat que vous pouvez utiliser est limité par les types de certificats pris en charge par les applications qui utiliseront le certificat. Les certificats RSA sont généralement pris en charge par toutes les applications qui utilisent des certificats. Cependant, les certificats EDDSA peuvent ne pas être pris en charge par les systèmes d'exploitation des ordinateurs, les navigateurs, ASDM ou Secure Client (services client sécurisés). Par exemple, vous devez utiliser un certificat RSA pour l'identité et l'authentification VPN d'accès à distance. Pour le VPN de site à site, où l'ASA est l'application qui utilise le certificat, EDDSA est pris en charge.
- Pour les ASA configurés en tant que serveurs ou clients CA, limitez la période de validité du certificat à une date antérieure à la date de fin recommandée, soit le 19 janvier 2038 à 03:14:08 UTC. Ces lignes directrices s'appliquent également aux certificats importés de fournisseurs tiers.

- L'ASA établit une connexion LDAP/SSL uniquement si l'un des critères de certification suivants est satisfait :
  - Le certificat du serveur LDAP est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA) et est valide.
  - Un certificat d'autorité de certification des serveurs émettant la chaîne est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA), et tous les certificats d'autorité de certification subordonnés de la chaîne sont complets et valides.
- Lorsqu'une inscription de certificat est terminée, l'ASA stocke un fichier PKCS12 contenant la paire de clés et la chaîne de certificat de l'utilisateur, ce qui nécessite environ 2 Ko de mémoire flash ou d'espace disque par inscription. La quantité réelle d'espace disque dépend de la configuration de la clé RSA et des champs de certificat. Gardez ces lignes directrices à l'esprit lors de l'ajout d'un grand nombre d'inscriptions de certificat en attente sur un ASA avec une quantité limitée de mémoire flash disponible, car ces fichiers PKCS12 sont stockés dans la mémoire flash pendant toute la durée du délai d'expiration de récupération de l'inscription configuré. Nous vous conseillons d'utiliser une taille de clé d'au moins 2048.
- Vous devez configurer l'ASA pour utiliser un certificat d'identité afin de protéger le trafic ASDM et le trafic HTTPS vers l'interface de gestion. Les certificats d'identité qui sont automatiquement générés avec SCEP sont régénérés après chaque redémarrage, alors assurez-vous d'installer manuellement vos propres certificats d'identité. Pour obtenir un exemple de cette procédure qui s'applique uniquement à SSL, consultez l'URL suivante : http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml.
- L'ASA et le Secure Client (services client sécurisés) ne peuvent valider que les certificats dans lesquels le champ X520Serialnumber (numéro de série dans le nom d'objet) est au format PrintableString. Si le format du numéro de série utilise un encodage tel que UTF8, l'autorisation de certificat échouera.
- Utilisez uniquement des caractères et des valeurs valides pour les paramètres de certificat lorsque vous les importez sur l'ASA. Dans l'ASA, ces certificats sont décodés afin d'être intégrés dans des structures de données internes. Les certificats comportant des champs vides sont interprétés comme non conformes aux normes de décodage et, par conséquent, la validation de l'installation échoue. Cependant, à partir de la version 9.16, les valeurs vides des champs facultatifs n'ont aucune incidence sur les critères de décodage et de validation d'installation.
- Pour utiliser un caractère générique (*), assurez-vous d'utiliser l'encodage sur le serveur CA qui autorise ce caractère dans la valeur de chaîne. Bien que la RFC 5280 recommande d'utiliser un UTF8String ou PrintableString, vous devez utiliser UTF8String, car PrintableString ne reconnaît pas le caractère générique comme un caractère valide. L'ASA rejette le certificat importé si un caractère ou une valeur non valide est détecté pendant l'importation. Par exemple :

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕv°3é¼p0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

- Configurez le serveur DNS sur le périphérique pour une inscription ACME réussie. Pour en savoir plus sur la procédure de configuration du serveur DNS, consultez Configurer des serveurs DNS, à la page 844.

Configurer les certificats numériques

Les rubriques suivantes expliquent comment configurer les certificats numériques.

Configurer les paires de clés

Pour créer ou supprimer des paires de clés, procédez comme suit.

Procédure

Étape 1 Générez une paire de clés RSA par défaut à usage général.

crypto key generate rsa modulus 2048

Exemple :

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

Le module de clé par défaut est 2048, mais vous devez spécifier explicitement le module pour vous assurer d'obtenir la taille dont vous avez besoin. La clé s'appelle Default-RSA-Key.

Pour les clés RSA, le module peut être l'un des éléments suivants (en bits) : 2 048 ou.

Si vous souhaitez également une clé d'algorithme de signature à courbe elliptique (ECDSA), vous pouvez générer la clé Default-ECDSA-Key. La longueur par défaut est de 384, mais vous pouvez également utiliser 256 ou 521.

crypto key generate ecdsa elliptic-curve 384

Si vous souhaitez également une clé d'algorithme de signature à courbe d'Edwards (EdDSA), vous pouvez générer la clé Default-EdDSA-Key. La longueur par défaut est de 256 bits.

Remarque
Les inscriptions EST sur l'ASA à l'aide de paires de clés de type EdDSA (Ed25519) ne sont pas prises en charge. Les inscriptions EST ne peuvent utiliser que des clés RSA ou ECDSA.

crypto key generate eddsa edward-curve Ed25519

Étape 2 (Facultatif) Créez des clés supplémentaires avec des noms uniques.

crypto key generate rsa label *key-pair-label* **modulus** *size*

crypto key generate ecdsa label *key-pair-label* **elliptic-curve** *size*

Exemple :

```
ciscoasa(config)# crypto key generate rsa label exchange modulus 2048
```

L'étiquette est référencée par le point de confiance qui utilise la paire de clés.

Étape 3 Vérifiez les paires de clés que vous avez générées.

show crypto key mypubkey {**rsa** | **ecdsa**}

Exemple :

```
ciscoasa/contexta(config)# show crypto mypubkey key rsa
```

Étape 4 Enregistrez la paire de clés que vous avez générée.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Étape 5 Si nécessaire, supprimez les paires de clés existantes afin de pouvoir en générer de nouvelles.

crypto key zeroize {**rsa** | **ecdsa**}

Exemple :

```
ciscoasa(config)# crypto key zeroize rsa
```

Étape 6 (Facultatif) Archivez le certificat et la paire de clés du serveur CA local.

copy

Exemple :

```
ciscoasa# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/
```

Cette commande copie le certificat et la paire de clés du serveur CA local ainsi que tous les fichiers de l'ASA à l'aide de FTP ou de TFTP.

Remarque
Assurez-vous de sauvegarder tous les fichiers du serveur CA local aussi souvent que possible.

Étape 7 Pour les méthodes d'inscription qui prennent en charge l'inscription automatique, des paires de clés sont automatiquement générées et stockées dans la mémoire flash au moment de l'inscription. Pour activer cette prise en charge, les paramètres clés suivants sont spécifiés dans le point de confiance :

L'exemple suivant montre la configuration de la paire de clés ECDSA :

```
ciscoasa(config-ca-trustpoint)# keypair ?

crypto-ca-trustpoint mode commands/options:
  WORD < 129 char  Name of key pair
  ecdsa            Generate ECDSA keys
  eddsa            Generate EDDSA keys
  rsa              Generate RSA keys
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve ?

crypto-ca-trustpoint mode commands/options:
  256  256 bits
  384  384 bits
  521  521 bits
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve 521
ciscoasa(config-ca-trustpoint)#
```

L'exemple suivant montre la configuration de la paire de clés RSA :

```
ciscoasa(config-ca-trustpoint)# keypair ?

crypto-ca-trustpoint mode commands/options:
  WORD < 129 char  Name of key pair
  ecdsa            Generate ECDSA keys
  eddsa            Generate EDDSA keys
  rsa              Generate RSA keys
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve ?

ciscoasa(config-ca-trustpoint)# keypair rsa modulus ?

crypto-ca-trustpoint mode commands/options:
  2048  2048 bits
  3072  3072 bits
  4096  4096 bits
ciscoasa(config-ca-trustpoint)# keypair rsa modulus 2048
ciscoasa(config-ca-trustpoint)#
```

Étape 8 Vous pouvez supprimer les paires de clés en exécutant la commande suivante :

crypto key zeroize rsa

L'exemple suivant montre comment supprimer des paires de clés :

Exemple :

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
```

Configurer les points de confiance

Pour configurer un point de confiance, procédez comme suit :

Procédure

Étape 1 Créez un point de confiance qui correspond à la CA à partir de laquelle l'ASA doit recevoir un certificat.

crypto ca trustpoint *trustpoint-name*

Exemple :

```
ciscoasa/contexta(config)# crypto ca trustpoint Main
```

Vous entrez en mode de configuration du point de confiance de la CA de chiffrement, qui contrôle les paramètres de point de confiance spécifiques à la CA que vous pouvez configurer à partir de l'étape 3.

Étape 2 Précisez l'interface source pour la certification CA :

enrollment interface *interface-name*

```
ciscoasa(config-ca-trustpoint)#  enrollment interface mgmt
```

Étape 3 Choisissez une des options suivantes :

- Demandez l'inscription automatique à l'aide de SCEP avec le point de confiance spécifié et configurez l'URL d'inscription en exécutant la commande suivante :

  enrollment protocol scep *url*

  Exemple :

  ```
  ciscoasa/contexta(config-ca-trustpoint)# enrollment protocol scep url
  http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

- Demandez l'inscription automatique à l'aide de CMP avec le point de confiance spécifié et configurez l'URL d'inscription en exécutant la commande suivante :

  enrollment protocol cmp *url*

  Exemple

  ```
  ciscoasa/ contexta(config-ca-trustpoint)# enrollment protocol cmp url
  http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

  Remarque
  La licence de l'opérateur doit être incluse pour permettre l'inscription au CMP.

- Demandez l'inscription manuelle avec le point de confiance spécifié en collez le certificat reçu de la CA au terminal en exécutant la commande suivante :

  enrollment terminal

  ```
  ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal
  ```

- Demandez un certificat autosigné en exécutant la commande suivante :

  enrollment self

- Demandez l'inscription automatique à l'aide d'EST avec le point de confiance spécifié et configurez l'URL d'inscription en exécutant la commande suivante :

  enrollment protocol est *url*

  Exemple

  ```
  asa(config-ca-trustpoint)# enrollment protocol est ?

  crypto-ca-trustpoint mode commands/options:
    url CA server enrollment URL
  asa(config-ca-trustpoint)# enrollment protocol est url ?
   crypto-ca-trustpoint mode commands/options:
    LINE < 477 char  URL
  asa(config-ca-trustpoint)# enrollment protocol est url https://xyz.com/est
  ```

Étape 4 Si le point de confiance a été configuré pour utiliser CMP à l'étape ci-dessus, vous pouvez éventuellement activer la fonctionnalité qui demande automatiquement des certificats. Saisissez un pourcentage de la durée de vie absolue du certificat, après quoi l'inscription automatique sera nécessaire et précisez si vous souhaitez générer une nouvelle clé lors du renouvellement du certificat.

```
[no] auto-enroll [<percent>] [regenerate]
```

Étape 5 Spécifiez les options de configuration CRL disponibles.

revocation-check crl none

Remarque
La commande **revocation-check crl none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl
ciscoasa/contexta(config-ca-trustpoint)# revocation-check none
```

Remarque
Pour activer la vérification CRL requise ou facultative, assurez-vous de configurer le point de confiance pour la gestion des CRL après l'obtention des certificats.

Étape 6 Activez ou désactivez l'extension des contraintes de base et l'indicateur CA.

[**no**]**ca-check**

L'extension des contraintes de base détermine si le sujet du certificat est une autorité de certification (CA), auquel cas le certificat peut être utilisé pour signer d'autres certificats. L'indicateur de d'autorité de certification fait partie de cette extension. La présence de ces éléments dans un certificat indique que la clé publique du certificat peut être utilisée pour valider les signatures de certificat.

La commande **ca-check** est activée par défaut. Vous ne devez donc saisir cette commande que si vous souhaitez désactiver les contraintes de base et l'indicateur CA.

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# no ca-check
```

Étape 7 Lors de l'inscription, demandez à la CA d'inclure l'adresse courriel spécifiée dans l'extension de nom alternatif du sujet du certificat.

email *address*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# email example.com
```

Étape 8 (Facultatif) Spécifiez une période de nouvelle tentative en minutes, applicable uniquement à l'inscription SCEP.

enrollment retry period

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5
```

Étape 9 (Facultatif) Spécifiez un nombre maximum de nouvelles tentatives autorisées, applicable uniquement à l'inscription SCEP.

enrollment retry count

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2
```

Étape 10 Lors de l'inscription, demandez à la CA d'inclure le nom de domaine complet spécifié dans l'extension de nom alternatif du sujet du certificat.

fqdn *fqdn*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com
```

Étape 11 Lors de l'inscription, demandez à la CA d'inclure l'adresse IP de l'ASA dans le certificat.

ip-address *ip-address*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1
```

Étape 12 Spécifiez la paire de clés dont la clé publique doit être certifiée.

keypair *name*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# keypair exchange
```

Étape 13 Si vous avez des points de confiance configurés pour CMP, déterminez si vous souhaitez générer des clés EDDSA, des clés EDCSA ou des clés RSA pour des inscriptions manuelles et automatiques.

```
no keypair name | [rsa modulus 2048|4096] | [edcsa elliptic-curve 256|384|521] | [ eddsa
edwards-curve Ed25519 ]
```

Remarque
Les inscriptions EST sur l'ASA à l'aide de paires de clés de type EDDSA (Ed25519) ne sont pas prises en charge. Les inscriptions EST ne peuvent utiliser que des clés RSA et ECDSA. L'inscription à ACME avec le type de paire de clés EDDSA n'est pas prise en charge.

Remarque
Lorsque le groupe de chiffrement ECDHE_ECDSA est utilisé, configurez le point de confiance avec un certificat contenant une clé compatible avec ECDSA. Les certificats avec une clé RSA ne sont pas compatibles avec les chiffrements ECDSA.

Étape 14 Configurez les remplacements d'URL OCSP et les points de confiance à utiliser pour la validation des certificats de répondeur OCSP.

match certificate map-name override ocsp

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp
```

Étape 15 Configurez l'interface source pour que l'ASA atteigne le protocole OCSP :

interface *nameif*

Exemple :

```
ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  interface      Configure Source interface
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp  interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
  inside   Name of interface GigabitEthernet0/0.100
  inside1  Name of interface GigabitEthernet0/0.41
  mgmt     Name of interface Management0/0
  outside  Name of interface GigabitEthernet0/0.51
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
```

Étape 16 Désactivez l'extension de nonce sur une requête OCSP. L'extension de nonce lie cryptographiquement les requêtes aux réponses pour éviter les attaques par relecture.

ocsp disable-nonce

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce
```

Étape 17 Configurez un serveur OCSP que l'ASA utilisera pour vérifier tous les certificats associés à un point de confiance plutôt que le serveur spécifié dans l'extension AIA du certificat client.

ocsp url

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp url
```

Étape 18 Spécifiez une phrase de défi enregistrée auprès de la CA lors de l'inscription. La CA utilise généralement cette phrase pour authentifier une demande de révocation ultérieure.

password *string*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# password mypassword
```

Étape 19 Définissez une ou plusieurs méthodes pour la vérification de la révocation : CRL, OCSP et Aucune.

Remarque
Lorsque vous affectez une URL OCSP pour la vérification de la révocation, vous pouvez spéficier l'interface (y compris l'interface de gestion) à partir de laquelle l'OCSP est accessible. Cette valeur d'interface détermine la décision de routage.

revocation check

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# revocation check
```

Étape 20 Lors de l'inscription, demandez à la CA d'inclure le DN du sujet spécifié dans le certificat. Si une chaîne de nom distinctif comprend une virgule, incluez la chaîne de valeur entre guillemets doubles (par exemple, O= « Société, Inc. »).

subject-name *X.500 name*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename
```

Étape 21 Lors de l'inscription, demandez à la CA d'inclure le numéro de série de l'ASA dans le certificat.

serial-number

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7
```

Étape 22 Enregistrez la configuration en cours d'exécution.

write memory

Exemple :

```
ciscoasa/contexta(config)# write memory
```

Configurer les CRL pour un point de confiance

Pour utiliser la vérification des CRL obligatoires ou facultatives lors de l'authentification par certificat, vous devez configurer les CRL pour chaque point de confiance. Pour configurer les CRL pour un point de confiance, procédez comme suit :

Procédure

Étape 1 Entrez dans le mode de configuration du point de confiance CA cryptographique pour accéder au point de confiance dont vous souhaitez modifier la configuration des CRL.

crypto ca trustpoint *trustpoint-name*

Exemple :

```
ciscoasa (config)# crypto ca trustpoint Main
```

Remarque

Assurez-vous d'avoir activé les CRL avant de saisir cette commande. En outre, la CRL doit être disponible pour que l'authentification réussisse.

Étape 2 Entrez dans le mode de configuration de CRL pour le point de confiance actuel.

crl configure

Exemple :

```
ciscoasa(config-ca-trustpoint)# crl configure
```

Astuces
Pour définir tous les paramètres de configuration de CRL aux valeurs par défaut, utilisez la commande **default**. À tout moment pendant la configuration de la CRL, saisissez à nouveau cette commande pour redémarrer la procédure.

Étape 3 Choisissez l'une des options suivantes pour configurer la politique de récupération :

- Les CRL sont extraites uniquement des URL des points de distribution de CRL (CDP) spécifiées dans les certificats authentifiés.

  policy cdp

  ```
  ciscoasa(config-ca-crl)# policy cdp
  ```

  Remarque
  La récupération SCEP n'est pas prise en charge par les points de distribution spécifiés dans les certificats.

- Les CRL sont extraites uniquement de la règle de correspondance de la carte de certificat que vous configurez.

  policy static

  ```
  ciscoasa(config-ca-crl)# policy static
  ```

- Les CRL sont extraites des points de distribution de CRL spécifiés dans les certificats authentifiés et de la règle de correspondance de la carte de certificat que vous configurez.

  policy both

  ```
  ciscoasa(config-ca-crl)# policy both
  ```

Étape 4 Si vous avez utilisé les mots clés **static** ou **both** lors de la configuration de la politique de CRL, vous devez configurer la règle de correspondance de la carte de certificat pour la récupération des CRL. Vous pouvez désormais configurer plusieurs CDP statiques sur une seule carte.

enrollment terminal

Pour supprimer une instance en particulier, sous la forme **no** de la commande, incluez le numéro de séquence ou l'URL. Assurez-vous que les valeurs spécifiées correspondent aux valeurs configurées. Pour supprimer toutes les entrées de la carte, utilisez simplement la commande **no**.

Exemple :

```
ciscoasa(crypto ca trustpoint)#enrollment terminal

ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  10 url http://192.0.2.10
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  20 url http://192.0.2.12
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  30 url http://192.0.2.13
```

Étape 5 Précisez HTTP, LDAP ou SCEP comme méthode de récupération des CRL.

protocol http | **ldap** | **scep**

Exemple :

```
ciscoasa(config-ca-crl)# protocol http
```

Étape 6 Configurez la durée pendant laquelle l'ASA met en cache les CRL pour le point de confiance actuel. L'argument *refresh-time* est le nombre de minutes que l'ASA attend avant de prendre en compte une CRL obsolète.

cache-time *refresh-time*

Exemple :

```
ciscoasa(config-ca-crl)# cache-time 420
```

Étape 7 Effectuez l'une des opérations suivantes :

- Exigez la présence du champ NextUpdate dans les CRL. Il s'agit du paramètre par défaut.

  enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# enforcenextupdate
  ```

- Permettez au champ NextUpdate d'être absent des CRL.

  no enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# no enforcenextupdate
  ```

Étape 8 Identifiez le serveur LDAP à l'ASA si LDAP est spécifié comme protocole de récupération. Vous pouvez spécifier le serveur par nom de domaine DNS ou par adresse IP. Vous pouvez également fournir un numéro de port si le serveur écoute les requêtes LDAP sur un port autre que la valeur par défaut de 389.

ldap-defaults *server*

Exemple :

```
ciscoasa (config-ca-crl)# ldap-defaults ldap1
```

Remarque
Si vous utilisez un nom de domaine au lieu d'une adresse IP pour spécifier le serveur LDAP, assurez-vous d'avoir configuré l'ASA pour utiliser DNS.

Étape 9 Autorisez la récupération de la CRL si le serveur LDAP requiert des informations d'authentification.

ldap-dn *admin-DN password*

Exemple :

```
ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c001RunZ
```

Étape 10 Récupérez la CRL actuelle de la CA représentée par le point de confiance spécifié et testez la configuration de la CRL pour le point de confiance actuel.

crypto ca crl request *trustpoint*

Exemple :

```
ciscoasa (config-ca-crl)# crypto ca crl request Main
```

Étape 11 Enregistrez la configuration en cours d'exécution.

write memory

Exemple :

```
ciscoasa (config)# write memory
```

Exporter ou importer une configuration de point de confiance

Pour exporter et importer une configuration de point de confiance, procédez comme suit :

Procédure

Étape 1 Exportez une configuration de point de confiance avec toutes les clés et tous les certificats associés au format PKCS12.

crypto ca export *trustpoint*

Exemple :

```
ciscoasa(config)# crypto ca export Main
```

L'ASA affiche les données PKCS12 dans le terminal. Vous pouvez copier les données. Les données du point de confiance sont protégées par un mot de passe. Toutefois, si vous enregistrez les données du point de confiance dans un fichier, assurez-vous que celui-ci se trouve dans un emplacement sécurisé.

Étape 2 Importez les paires de clés et les certificats émis qui sont associés à une configuration de point de confiance.

crypto ca import *trustpoint* **pkcs12***passphrase*

Exemple :

```
ciscoasa(config)# crypto ca import Main pkcs12 ?
```

L'ASA vous invite à coller le texte dans le terminal au format base 64. Une étiquette correspondant au nom du point de confiance que vous créez est attribuée à la paire de clés importée avec le point de confiance.

Remarque
Si un ASA dispose de points de confiance qui partagent la même CA, vous ne pouvez utiliser qu'un seul des points de confiance qui partagent la CA pour valider les certificats d'utilisateur. Pour contrôler le partage du point de confiance qu'une CA utilise pour la validation des certificats d'utilisateur émis par cette CA, utilisez le mot clé **support-user-cert-validation**.

Exemples

L'exemple suivant exporte les données PKCS12 pour le point de confiance principal avec la phrase secrète Wh0zits :

```
ciscoasa(config)# crypto ca export Main pkcs12 Wh0zits

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

L'exemple suivant importe manuellement les données PKCS12 dans le point de confiance principal avec la phrase secrète Wh0zits :

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

Dans l'exemple suivant, un certificat est importé manuellement pour le point de confiance principal :

```
ciscoasa (config)# crypto ca import Main certificate
% The fully qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

Configurer les règles de mappage des certificats CA

Vous pouvez configurer des règles en fonction des champs Issuer (Émetteur) et Subject (Sujet) d'un certificat. En utilisant les règles que vous créez, vous pouvez mapper les certificats d'homologues IPsec aux groupes de tunnels à l'aide de la commande **tunnel-group-map**.

Pour configurer une règle de mappage de certificat CA, procédez comme suit :

Procédure

Étape 1 Entrez dans le mode de configuration de la carte de certificat CA pour la règle que vous souhaitez configurer et précisez le numéro de séquence de la règle.

crypto ca certificate map [*map_name*]*sequence-number*

Exemple :

```
ciscoasa(config)# crypto ca certificate map test-map 10
```

Si vous ne spécifiez pas le nom de la carte, la règle est ajoutée à la carte par défaut : DefaultCertificateMap. Pour chaque numéro de règle, vous pouvez spécifier un ou plusieurs champs à faire correspondre.

Étape 2 Spécifiez le nom de l'émetteur ou le nom du sujet :

{**issuer-name** | **subject-name**} [**attr** *attribute*] *operator string*

Exemple :

```
ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr uid eq jcrichton
```

Vous pouvez faire correspondre la valeur complète ou spécifier les attributs que vous souhaitez faire correspondre. Les attributs suivants sont valides :

- c : pays
- cn : nom commun
- dc : composant de domaine
- dnq : qualificateur de nom distinctif
- emailAddress : adresse courriel
- genq : qualificatif générationnel
- gn : prénom
- i : initiales
- ip : adresse IP
- l : localité
- n : nom
- o : nom de l'organisation
- ou : unité organisationnelle
- ser : numéro de série

Remarque

Assurez-vous de spécifier l'attribut de numéro de série dans le nom d'objet. Le mappage de certificat correspond uniquement à un attribut de numéro de série spécifié dans le nom d'objet.

- sn : nom de famille
- sp : État/province
- t : titre
- uid : ID d'utilisateur
- uname : nom non structuré

Voici des opérateurs valides :

- eq : le champ ou l'attribut doit être identique à la valeur donnée.
- ne : le champ ou l'attribut ne peut pas être identique à la valeur attribuée.
- co : une partie ou la totalité du champ ou de l'attribut doit correspondre à la valeur donnée.
- nc : aucune partie du champ ou de l'attribut ne peut correspondre à la valeur donnée.

Étape 3 Spécifiez l'autre nom d'objet :

alt-subject-name *operator string*

Exemple :

```
ciscoasa(config-ca-cert-map)# alt-subject-name eq happydays
```

Voici des opérateurs valides :

- eq : le champ doit être identique à la valeur donnée.
- ne : le champ ne peut pas être identique à la valeur donnée.
- co : une partie ou la totalité du champ doit correspondre à la valeur donnée.
- nc : aucune partie du champ ne peut correspondre à la valeur donnée.

Étape 4 Spécifiez l'utilisation de la clé étendue :

extended-key-usage *operator OID_string*

Exemple :

```
ciscoasa(config-ca-cert-map)# extended-key-usage nc clientauth
```

Voici des opérateurs valides :

- co : une partie ou la totalité du champ doit correspondre à la valeur donnée.
- nc : aucune partie du champ ne peut correspondre à la valeur donnée.

Voici des chaînes OID valides :

- *string* : chaîne définie par l'utilisateur.

- clientauth : authentification du client (1.3.6.1.5.5.7.3.2)
- codesigning : signature de code (1.3.6.1.5.5.7.3.3)
- emailprotection – Secure Email Protection (1.3.6.1.5.5.7.3.4)
- ocspsigning : signature OCSP (1.3.6.1.5.5.7.3.9)
- serverauth : authentification du serveur (1.3.6.1.5.5.7.3.1)
- timestamping : horodatage (1.3.6.1.5.5.7.3.8)

Configurer les identités de référence

Lorsque l'ASA agit en tant que client TLS, il prend en charge les règles de vérification de l'identité d'un serveur d'applications, comme défini dans la RFC 6125. Cette RFC spécifie les procédures pour représenter les identités de référence (configurées sur l'ASA) et les vérifier par rapport aux identités présentées (envoyées par le serveur d'applications). Si l'identité présentée ne peut pas être comparée à l'identité de référence configurée, la connexion n'est pas établie et une erreur est enregistrée.

Le serveur présente son identité en incluant un ou plusieurs identifiants dans le certificat de serveur présenté à l'ASA lors de l'établissement de la connexion. Les identités de référence sont configurées sur l'ASA pour être comparées à l'identité présentée dans un certificat de serveur lors de l'établissement de la connexion. Ces identifiants sont des instances spécifiques des quatre types d'identifiants spécifiés dans la RFC 6125. Les quatre types d'identifiants sont les suivants :

- CN_ID : nom distinctif relatif (RDN) dans un champ d'objet de certificat qui ne contient qu'une seule paire d'attributs types et de valeurs de type de nom commun (CN), dans lequel la valeur correspond à la forme globale d'un nom de domaine. La valeur CN ne peut pas être en texte libre. Un identifiant de référence CN-ID n'identifie pas un service d'application.
- DNS-ID : une entrée subjectAltName de type dNSName. Il s'agit d'un nom de domaine DNS. Un identifiant de référence DNS-ID n'identifie pas un service d'application.
- SRV-ID : une entrée subjectAltName de type otherName dont le format de nom est SRVName comme défini dans la RFC 4985. Un identifiant SRV-ID peut contenir à la fois un nom de domaine et un type de service d'application. Par exemple, un SRV-ID de « _imaps.example.net » serait divisé en une partie de nom de domaine DNS de « example.net » et une partie de type de service d'application de « imaps ».
- URI-ID : Une entrée subjectAltName de type uniformResourceIdentifier dont la valeur comprend à la fois (i) un schéma et (ii) un composant « hôte » (ou son équivalent) qui correspond à la règle « reg-name » spécifiée dans la RFC 3986. Un identifiant URI-ID doit contenir le nom de domaine DNS, pas l'adresse IP et pas seulement le nom d'hôte. Par exemple, un URI-ID de « sip:voice.example.edu » serait divisé en une partie de nom de domaine DNS de « voice.example.edu » et un type de service d'application de « sip ».

Une identité de référence est créée lors de la configuration d'une identité avec un nom précédemment inutilisé. Une fois qu'une identité de référence a été créée, les quatre types d'identifiants et leurs valeurs associées peuvent être ajoutés ou supprimés de l'identité de référence. Les identifiants de référence PEUVENT contenir des renseignements identifiant le service d'application et doivent contenir des renseignements identifiant le nom de domaine DNS.

Avant de commencer

- Les identités de référence sont utilisées lors de la connexion au serveur de journal système et au serveur de licences Smart uniquement. Aucune autre connexion en mode client SSL ASA ne prend actuellement en charge la configuration ou l'utilisation des identités de référence.
- L'ASA met en œuvre toutes les règles de correspondance des identifiants décrites dans la RFC 6125, à l'exception des certificats épinglés et du système de secours pour les clients interactifs.
- La possibilité d'épingler des certificats n'est pas mise en œuvre. Par conséquent, `aucune correspondance n'a été trouvée, le certificat épinglé` ne se produira pas. De plus, un utilisateur n'aura pas la possibilité d'épingler un certificat si aucune correspondance n'est trouvée, car notre mise en œuvre n'est pas un client interactif.

Procédure

Étape 1 Saisissez la commande **[no] crypto ca reference-identity** dans le mode de configuration globale pour placer l'ASA en mode ca-reference-identity.

[no] crypto ca reference-identity *reference-identity-name*

Si aucune identité de référence avec ce *reference-identity-name* n'est trouvée, une nouvelle identité de référence est créée. Si la forme **no** de la commande est exécutée pour une identité de référence toujours utilisée, un avertissement s'affiche et l'identité de référence n'est pas supprimée.

Étape 2 Saisissez les ID de référence en mode ca-reference-identity. Plusieurs identifiants de référence de tout type peuvent être ajoutés à l'identité de référence.

- **[no] cn-id** *value*
- **[no] dns-id** *value*
- **[no] srv-id** *value*
- **[no] uri-id** *value*

Pour supprimer une identité de référence, utilisez la forme no de la commande.

Exemple

Configurez une identité de référence pour la validation du certificat de serveur RFC 6125 pour un serveur de journal système :

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

Prochaine étape

Utilisez l'identité de référence lors de la configuration des connexions du journal système et du serveur Smart Call Home.

Obtenir des certificats manuellement

Pour obtenir des certificats manuellement, procédez comme suit :

Avant de commencer

Vous devez déjà avoir obtenu un certificat CA codé en base-64 auprès de la CA représentée par le point de confiance.

Procédure

Étape 1 Importez le certificat CA pour le point de confiance configuré.

crypto ca authenticate *trustpoint*

Exemple :

```
ciscoasa(config)# crypto ca authenticate Main
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[ certificate data omitted ]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint:     24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

L'utilisation de la commande **enrollment terminal** lors de la configuration du point de confiance requiert que vous obteniez manuellement des certificats.

Étape 2 Inscrivez l'ASA auprès du point de confiance.

crypto ca enroll *trustpoint*

Exemple :

```
ciscoasa(config)# crypto ca enroll Main
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: securityappliance.example.com

% Include the device serial number in the subject name? [yes/no]: n

Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t
[ certificate request data omitted ]
jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt

---End - This line not part of the certificate request---
```

```
Redisplay enrollment request? [yes/no]: n
```

Cette commande génère un certificat pour la signature des données et, en fonction du type de clés que vous avez configuré, pour le chiffrement des données. Si vous utilisez des clés RSA distinctes pour la signature et le chiffrement, la commande **crypto ca enroll** affiche deux demandes de certificat, une pour chaque clé. Si vous utilisez des clés RSA à usage général pour la signature et le chiffrement, la commande **crypto ca enroll** affiche une demande de certificat.

Pour terminer l'inscription, procurez-vous un certificat pour toutes les demandes de certificat générées par la commande **crypto ca enroll** auprès de la CA représentée par le point de confiance applicable. Assurez-vous que le certificat est au format base-64.

Étape 3 Lorsqu'un point de confiance est configuré pour CMP, il est possible de spécifier une valeur secrète partagée (ir) ou le nom du point de confiance qui contient le certificat qui signera la demande (cr), mais pas les deux. Fournissez une valeur hors bande par la CA qui est utilisée pour confirmer l'authentification et l'intégrité des messages échangés avec l'ASA ou fournissez le nom du point de confiance avec un certificat d'appareil précédemment émis et utilisé pour signer la demande d'inscription CMP. Les mots clés de secrets partagés ou de certificats de signature ne sont disponibles que lorsque le protocole d'inscription du point de confiance est défini sur CMP.

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

Étape 4 Déterminez si une nouvelle paire de clés doit être générée ou non avant de créer la demande d'inscription.

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

Étape 5 Importez chaque certificat que vous recevez de la CA et assurez-vous de coller le certificat dans le terminal au format base-64.

crypto ca import *trustpoint* **certificate**

Exemple :

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

Étape 6 Vérifiez que le processus d'inscription a réussi en affichant les détails du certificat émis pour l'ASA et le certificat CA pour le point de confiance.

show crypto ca certificate

Exemple :

```
ciscoasa(config)# show crypto ca  certificate Main
```

Étape 7 Enregistrez la configuration en cours d'exécution.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Étape 8 Répétez ces étapes pour chaque point de confiance que vous configurez pour l'inscription manuelle.

Obtenir des certificats automatiquement avec SCEP

Cette section décrit comment obtenir automatiquement des certificats en utilisant SCEP.

Avant de commencer

Vous devez déjà avoir obtenu un certificat CA codé en base-64 auprès de la CA représentée par le point de confiance.

Procédure

Étape 1 Obtenez le certificat CA pour le point de confiance configuré.

crypto ca authenticate *trustpoint*

Exemple :

```
ciscoasa/contexta(config)# crypto ca authenticate Main
```

Lorsque vous configurez le point de confiance, l'utilisation de la commande **enrollment url** détermine si vous devez obtenir les certificats automatiquement ou non par SCEP.

Étape 2 Inscrivez l'ASA auprès du point de confiance. Cette commande récupère un certificat pour la signature des données et, en fonction du type de clés que vous avez configuré, pour le chiffrement des données. Avant d'entrer cette commande, communiquez avec l'administrateur CA, qui devra peut-être authentifier la demande d'inscription manuellement avant que la CA n'accorde les certificats.

crypto ca enroll *trustpoint*

Exemple :

```
ciscoasa/contexta(config)# crypto ca enroll Main
```

Si l'ASA ne reçoit pas de certificat de la CA dans un délai d'une minute (par défaut) après l'envoi d'une demande de certificat, il renvoie la demande de certificat. L'ASA continue d'envoyer une demande de certificat chaque minute jusqu'à ce qu'un certificat soit reçu.

Si le nom de domaine complet configuré pour le point de confiance n'est pas identique au nom de domaine complet de l'ASA, y compris la casse des caractères, un avertissement s'affiche. Pour résoudre ce problème, quittez le processus d'inscription, apportez les corrections nécessaires et saisissez à nouveau la commande **crypto ca enroll**.

Remarque
Si l'ASA redémarre après que vous ayez lancé la commande **crypto ca enroll**, mais avant que vous ayez reçu le certificat, saisissez la commande **crypto ca enroll** et avisez l'administrateur CA.

Étape 3 Vérifiez que le processus d'inscription a réussi en affichant les détails du certificat émis pour l'ASA et le certificat CA pour le point de confiance.

show crypto ca certificate

Exemple :

```
ciscoasa/contexta(config)# show crypto ca certificate Main
```

Étape 4 Enregistrez la configuration en cours d'exécution.

write memory

Exemple :

```
ciscoasa/contexta(config)# write memory
```

Configurer la prise en charge du serveur mandataire pour les demandes SCEP

Pour configurer l'ASA afin d'authentifier les points terminaux d'accès à distance à l'aide d'autorités de certification tierces, procédez comme suit :

Procédure

Étape 1 Entrez le mode de configuration tunnel-group ipsec-attributes.

tunnel-group *nom* **ipsec-attributes**

Exemple :

```
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
```

Étape 2 Activez les services clients.

crypto ikev2 enable outside client-services port *portnumber*

Exemple :

```
ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services
```

Le numéro de port par défaut est 443.

Remarque
Cette commande est nécessaire uniquement si vous prenez en charge IKEv2.

Étape 3 Entrez dans le mode de configuration tunnel-group general-attributes.

tunnel-group *nom* **general-attributes**

Exemple :

```
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
```

Étape 4 Activez l'inscription SCEP pour le groupe de tunnels.

scep-enrollment enable

Exemple :

```
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this option.
```

Étape 5 Entrez dans le mode de configuration des attributs group-policy.

group-policy *nom* **attributes**

Exemple :

```
ciscoasa(config)# group-policy FirstGroup attributes
```

Étape 6 Inscrivez la CA SCEP pour la stratégie de groupe. Entrez cette commande une fois par stratégie de groupe pour prendre en charge un certificat numérique tiers.

scep-forwarding-url value *URL*

Exemple :

```
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
```

URL est l'URL SCEP sur la CA.

Étape 7 Fournissez un mot de passe secondaire commun lorsqu'aucun certificat n'est disponible pour la prise en charge WebLaunch du mandataire SCEP.

secondary-pre-fill-username clientless hide use-common-password *password*

Exemple :

```
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
use-common-password secret
```

Vous devez utiliser le mot clé **hide** pour prendre en charge le mandataire SCEP.

Par exemple, un certificat n'est pas disponible pour un terminal qui en demande un. Une fois que le terminal a le certificat, l'Secure Client (services client sécurisés) se déconnecte, puis se reconnecte à l'ASA pour bénéficier d'une politique DAP qui fournit un accès aux ressources de réseau interne.

Étape 8 Masquez le nom d'utilisateur prérempli secondaire pour les sessions VPN Secure Client (services client sécurisés).

secondary-pre-fill-username ssl-client hide use-common-password *password*

Exemple :

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
```

```
use-common-password secret
```

Malgré le mot clé **ssl-client** hérité des versions précédentes, utilisez cette commande pour prendre en charge les sessions Secure Client (services client sécurisés) qui utilisent IKEv2 ou SSL.

Vous devez utiliser le mot clé **hide** pour prendre en charge le mandataire SCEP.

Étape 9 Fournissez le nom d'utilisateur lorsqu'aucun certificat n'est disponible.

secondary-username-from-certificate {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]

Exemple :

```
ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN no-certificate-fallback
 cisco-secure-desktop machine-unique-id
```

Comment configurer des types de certificats spécifiques

Après avoir établi des certificats de confiance, vous pouvez commencer d'autres tâches fondamentales telles que l'établissement de certificats d'identité ou des configurations plus avancées telles que l'établissement de certificats CA local ou de signature de code.

Avant de commencer

Lisez les renseignements sur les certificats numériques et établissez des certificats de confiance. Les certificats CA sans clé privée sont utilisés par tous les protocoles VPN et webvpn, et sont configurés dans des points de confiance pour valider les certificats clients entrants. De même, un groupe de confiance est une liste de certificats de confiance utilisés par les fonctionnalités de webvpn pour valider les connexions mandataires aux serveurs https et pour valider le certificat smart-call-home.

Procédure

Une CA locale permet aux clients VPN d'inscrire des certificats directement auprès de l'ASA. Cette configuration avancée convertit l'ASA en une CA. Pour configurer les CA, consultez Certificats de l'autorité de certification (CA), à la page 918.

Prochaine étape

Configurez une alerte d'expiration de certificat ou surveillez les certificats numériques et l'historique de gestion des certificats.

Certificats de l'autorité de certification (CA)

Cette page vous permet de gérer les certificats CA. Les rubriques suivantes expliquent ce que vous pouvez faire.

Gestion du serveur CA

Configurer l'importation automatique des certificats de groupe de confiance

La licence Smart utilise l'infrastructure Smart Call Home. Lorsque l'ASA configure les rapports anonymes de Smart Call Home en arrière-plan, l'ASA crée automatiquement un point de confiance contenant le certificat de la CA qui a émis le certificat de serveur Call Home. L'ASA prend désormais en charge la validation du certificat si la hiérarchie d'émission du certificat de serveur change, sans avoir besoin de l'intervention du client pour ajuster les modifications à la hiérarchie des certificats. Vous pouvez automatiser la mise à jour de l'ensemble de groupes de confiance à des intervalles périodiques afin que Smart Call Home puisse rester actif si le certificat autosigné du serveur CA change. Cette fonctionnalité n'est pas prise en charge dans le cadre des déploiements à contextes multiples.

L'importation automatique des ensembles de certificat de confiance vous oblige à spécifier l'URL utilisée par l'ASA pour télécharger et importer le groupe. Utilisez la commande suivante pour que l'importation ait lieu quotidiennement à des intervalles réguliers avec l'URL Cisco par défaut et l'heure par défaut de 22 heures :

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

Vous pouvez également activer l'importation automatique avec une URL personnalisée à l'aide de la commande suivante :

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

Pour vous offrir plus de flexibilité pour définir les téléchargements en dehors des heures de pointe ou à d'autres moments pratiques, saisissez la commande suivante qui active l'importation avec une heure personnalisée :

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

La définition de l'importation automatique avec une URL personnalisée et une heure personnalisée nécessite la commande suivante :

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

Afficher l'état de la politique de groupe de confiance

Utilisez la commande suivante pour voir l'état actuel de la politique de groupe de confiance :

```
show crypto ca trustpool policy
```

Cette commande renvoie les renseignements suivants :

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
 State: Not in progress
 Last import result: Not attempted N/A
 Current Jitter: 0

Trustpool auto import statistics:
 Last import result: N/A
 Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy

 Trustpool revocation checking is disabled.
 CRL cache time: 60 seconds
```

```
 CRL next update field: required and enforced
 Auto import of trustpool is enabled
 Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
 Download time: 22:00:00

Policy Overrides:
 None configured
```

Effacer le groupe de confiance CA

Pour réinitialiser la politique de groupe de confiance à son état par défaut, utilisez la commande suivante :

```
clear configure crypto ca trustpool
```

Étant donné que l'importation automatique des certificats de point de confiance est désactivée par défaut, l'utilisation de cette commande désactive la fonctionnalité.

Définir une alerte d'expiration de certificat (pour les certificats d'identité ou CA)

L'ASA vérifie tous les certificats CA et d'ID des points de confiance pour déterminer leur expiration une fois toutes les 24 heures. Si un certificat est sur le point d'expirer, un journal système sera émis en tant qu'alerte.

Une interface de ligne de commande est fournie pour configurer les intervalles de rappel et de récurrence. Par défaut, les rappels commencent à 60 jours avant l'expiration et se répèteront tous les 7 jours. Vous pouvez configurer l'intervalle auquel les rappels sont envoyés et le nombre de jours avant l'expiration à laquelle la première alerte est envoyée en utilisant la commande suivante :

```
[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]
```

Quelle que soit la configuration des alertes, un rappel est envoyé chaque jour pendant la dernière semaine d'expiration. Les commandes **show** et **clear** suivantes ont également été ajoutées :

```
clear conf crypto ca alerts
show run crypto ca alerts
```

En plus du rappel de réabonnement, si un certificat déjà expiré est détecté dans la configuration, un journal système est généré une fois par jour pour rectifier la configuration en renouvelant le certificat ou en supprimant le certificat expiré.

Par exemple, supposons que les alertes d'expiration sont configurées pour commencer à 60 jours et se répètent ensuite tous les 6 jours. Si l'ASA est redémarré au bout de 40 jours, une alerte est envoyée ce jour-là et l'alerte suivante est envoyée le 36e jour.



Remarque La vérification de l'expiration n'est pas effectuée sur les certificats de groupe de confiance. Le point de confiance CA local est également traité comme un point de confiance normal pour la vérification de l'expiration.

Supervision des certificats numériques

Consultez les commandes suivantes pour superviser l'état du certificat numérique :

- **show crypto ca server**

  Cette commande affiche la configuration et l'état de la CA locale.

- **show crypto ca server cert-db**

  Cette commande affiche les certificats d'utilisateur émis par la CA locale.

- **show crypto ca server certificate**

  Cette commande affiche les certificats de la CA locale sur la console au format base 64 et le certificat de renouvellement, lorsqu'ils sont disponibles, y compris l'empreinte numérique du certificat de renouvellement pour la vérification du nouveau certificat lors de l'importation sur d'autres périphériques.

- **show crypto ca server crl**

  Cette commande affiche les CRL.

- **show crypto ca server user-db**

  Cette commande affiche les utilisateurs et leur état. Elle peut être utilisée avec les qualificateurs suivants pour réduire le nombre d'enregistrements affichés :

  - allowed. Affiche uniquement les utilisateurs actuellement autorisés à s'inscrire.
  - enrolled. Affiche uniquement les utilisateurs inscrits et titulaires d'un certificat valide.
  - expired. Affiche uniquement les utilisateurs titulaires de certificats expirés.
  - on-hold. Répertorie uniquement les utilisateurs sans certificat et qui ne sont actuellement pas autorisés à s'inscrire.

- **show crypto ca server user-db allowed**

  Cette commande affiche les utilisateurs admissibles à l'inscription.

- **show crypto ca server user-db enrolled**

  Cette commande affiche les utilisateurs inscrits disposant de certificats valides.

- **show crypto ca server user-db expired**

  Cette commande affiche les utilisateurs disposant de certificats expirés.

- **show crypto ca server user-db on-hold**

  Cette commande affiche les utilisateurs sans certificat qui ne sont pas autorisés à s'inscrire.

- **show crypto key** *name of key*

  Cette commande affiche les paires de clés que vous avez générées.

- **show running-config**

  Cette commande affiche les règles de mappage des certificats émis par la CA locale.

Exemples

L'exemple suivant montre une clé RSA à usage général :

```
ciscoasa/contexta(config)# show crypto key mypubkey rsa
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Storage: config
 Key Data:

  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
  00ea2c38 df9c606e ddb7b08a e8b0a1a8 65592d85 0711cac5 fceddee1 fa494297
  525fffc0 90da8a4c e696e44e 0646c661 48b3602a 960d7a3a 52dae14a 5f983603
  e1f33e40 a6ce04f5 9a812894 b0fe0403 f8d7e05e aea79603 2dcd56cc 01261b3e
  93bff98f df422fb1 2066bfa4 2ff5d2a4 36b3b1db edaebf16 973b2bd7 248e4dd2
  071a978c 6e81f073 0c4cd57b db6d9f40 69dc2149 e755fb0f 590f2da8 b620efe6
  da6e8fa5 411a841f e72bb8ea cf4bdb79 f4e57ff3 a940ce3b 4a2c7052 56c1d17b
  af8fe2e2 e58718c6 ed1da0f0 1c6f36eb 79eb1aeb f098b5c4 79e07658 a52d8c7a
  51ceabfb f8ade096 7217cf2d 3728077e 89441d89 9bf5f875 c8d2db39 c858bb7a
  7d020301 0001
```

L'exemple suivant montre la liste CRL de la CA locale :

```
ciscoasa(config)# show crypto ca server crl
Certificate Revocation List:
    Issuer: cn=xx5520-1-3-2007-1
    This Update: 13:32:53 UTC Jan 4 2010
    Next Update: 13:32:53 UTC Feb 3 2010
    Number of CRL entries: 2
    CRL size: 270 bytes
Revoked Certificates:
    Serial Number: 0x6f
    Revocation Date: 12:30:01 UTC Jan 4 2010
    Serial Number: 0x47
    Revocation Date: 13:32:48 UTC Jan 4 2010
```

L'exemple suivant montre un utilisateur en attente :

```
ciscoasa(config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
ciscoasa(config)#
```

L'exemple suivant montre la sortie de commande **show running-config**, dans laquelle s'affichent les règles de mappage des certificats émis par la CA locale :

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

Historique de gestion des certificats

Tableau 33 : Historique de gestion des certificats

Nom de la caractéristique	Versions de plateforme	Description
Certificate Management	7.0(1)	Les certificats numériques (y compris les certificats CA, les certificats d'identité et les certificats de signataire de code) fournissent une identification numérique pour l'authentification. Un certificat numérique contient des renseignements permettant d'identifier un appareil ou un utilisateur, tels que le nom, le numéro de série, l'entreprise, le service ou l'adresse IP. Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur. Les autorités de certification émettent des certificats numériques dans le contexte d'une PKI, qui utilise le chiffrement par clé publique ou par clé privée pour assurer la sécurité.
Certificate Management	7.2(1)	Nous avons introduit les commandes suivantes : **issuer-name** *DN-string*, **revocation-check crl none**, **revocation-check crl**, **revocation-check none**. Nous avons rendu obsolètes les commandes suivantes : **crl** {**required** | **optional** | **nocheck**}.
Certificate Management	8.0(2)	Nous avons introduit les commandes suivantes : **cdp-url**, **crypto ca server**, **crypto ca server crl issue**, **crypto ca server revoke** *cert-serial-no*, **crypto ca server unrevoke** *cert-serial-no*, **crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*], **crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**], **crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}, **crypto ca server user-db remove** *username*, **crypto ca server user-db show-otp** {*username* | **all-certholders** | **all-unenrolled**}, **crypto ca server user-db write**, [**no**] **database path** *mount-name directory-path*, **debug crypto ca server** [*level*], **lifetime** {**ca-certificate** | **certificate** | **crl**} *time*, **no shutdown**, **otp expiration** *timeout*, **renewal-reminder** *time*, **show crypto ca server**, **show crypto ca server cert-db** [**user** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*], **show crypto ca server certificate**, **show crypto ca server crl**, **show crypto ca server user-db** [**expired** | **allowed** | **on-hold** | **enrolled**], **show crypto key** *name of key*, **show running-config**, **shutdown**.

Nom de la caractéristique	Versions de plateforme	Description
Mandataire SCEP	v 8.4(1)	Nous avons introduit cette fonctionnalité, qui permet un déploiement sécurisé des certificats de périphérique à partir d'autorités de certification tierces. Nous avons introduit les commandes suivantes : **crypto ikev2 enable outside client-services port** *portnumber*, **scep-enrollment enable**, **scep-forwarding-url value** *URL*, **secondary-pre-fill-username clientless hide use-common-password** *password*, **secondary-pre-fill-username ssl-client hide use-common-password** *password*, **secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**].
Identités de référence	9.6(2)	Le traitement du client TLS prend désormais en charge les règles de vérification de l'identité de serveur définies dans la RFC 6125, section 6. La vérification de l'identité sera effectuée pendant la validation PKI pour les connexions TLS au serveur de journal système et au serveur de licences Smart uniquement. Si l'identité présentée ne correspond pas à l'identité de référence configurée, la connexion n'est pas établie. Nous avons ajouté ou modifié les commandes suivantes : **crypto ca reference-identity**, **logging host**, **call home profile destination address**
Serveur CA local	9.12(1)	Pour que le FQDN de l'URL d'inscription soit configurable au lieu d'utiliser le FQDN configuré de l'ASA, une nouvelle option d'interface de ligne de commande est introduite. Cette nouvelle option est ajoutée au mode smpt du serveur CA de chiffrement. Nous avons rendu obsolète le serveur CA local et le supprimerons dans une version ultérieure : lorsque l'ASA est configuré en tant que serveur CA local, il est en mesure d'émettre des certificats numériques, de publier des listes de révocation de certificats (CRL) et de révoquer en toute sécurité les certificats émis. Cette fonctionnalité a été abandonnée et, par conséquent, la commande du serveur CA de chiffrement l'a été aussi.
Serveur CA local	9.13(1)	Nous avons supprimé la prise en charge du serveur CA local. Ainsi, la commande **crypto ca server** et ses sous-commandes sont supprimées. Nous avons supprimé les commandes suivantes : **crypto ca server** et toutes ses sous-commandes.

Nom de la caractéristique	Versions de plateforme	Description
Modifications des commandes du point de distribution de la CRL	9.13(1)	Les commandes de configuration d'URL de CDP statiques sont supprimées et déplacées vers la commande de certificat correspondante. Commandes nouvelles ou modifiées : **crypto-ca-trustpoint crl** et **crl url** ont été supprimées avec d'autres logiques connexes. **match-certificate override-cdp** a été introduite.
Taille du cache de la CRL augmentée	9.13(1)	Pour éviter l'échec de téléchargements de CRL volumineux, la taille du cache a été augmentée et la limite du nombre d'entrées dans une CRL individuelle a été supprimée. • Augmentation de la taille totale du cache de la CRL à 16 Mo par contexte pour le mode de contexte multiple. • Augmentation de la taille totale du cache de la CRL à 128 Mo pour le mode de contexte unique.
Option de restauration des contrôles de validité du certificat de contournement	9.15(1)	L'option de contournement de la vérification de la révocation en raison de problèmes de connectivité avec le serveur CRL ou OCSP, qui avait été supprimée dans la version 9.13(1), a été rétablie. Commandes nouvelles ou modifiées : **revocation-check crl none**, **revocation-check ocsp none**, **revocation-check crl ocsp none** et **revocation-check ocsp crl none** ont été restaurées.
Modifications apportées aux commandes de certificat correspondantes pour prendre en charge l'URL du point de distribution de la CRL statique	9.15(1)	La commande de configuration d'URL de CDP statiques a permis aux CDP statiques d'être mappés de façon unique à chaque certificat d'une chaîne validée. Cependant, un seul de ces mappages était pris en charge pour chaque certificat. Cette modification permet aux CDP configurés de manière statique d'être mappés à une chaîne de certificats pour l'authentification. Commandes nouvelles ou modifiées : **match certificate** *map* **override cdp** *seq* **url** *url* and **no match certificate** *map* **override cdp** *seq* **url** *url*
Les modifications apportées à la paire de clés du point de confiance et à la clé de chiffrement génèrent des commandes	9.16(1)	La prise en charge des certificats avec des tailles de clé inférieures à 2 048 a été supprimée. Toute configuration utilisant des options de 512, 768 ou 1 024 bits est transférée vers la version 2 048 avec notification dûe. La prise en charge de l'utilisation de l'algorithme de hachage SHA1 pour la certification a été supprimée. **Remarque** La commande **crypto ca permit-weak-crypto** a été introduite pour remplacer ces restrictions. La nouvelle option de clé EDDSA a été ajoutée aux options RSA et ECDSA existantes.



CHAPITRE 26

Inspection ARP et table des adresses MAC

Ce chapitre décrit comment personnaliser la table des adresses MAC et configurer l'inspection ARP pour les groupes de ponts.

- À propos de l'inspection ARP et de la table des adresses MAC, à la page 925
- Paramètres d'usine, à la page 926
- Lignes directrices pour l'inspection ARP et la table d'adresses MAC, à la page 927
- Configurer l'inspection ARP et les autres paramètres ARP, à la page 927
- Personnaliser la table des adresses MAC pour les groupes de ponts, à la page 929
- Supervision de l'inspection ARP et de la table des adresses MAC, à la page 931
- Historique de l'inspection ARP et de la table des adresses MAC, à la page 932

À propos de l'inspection ARP et de la table des adresses MAC

Pour les interfaces d'un groupe de ponts, l'inspection ARP empêche une attaque « man-in-the-middle ». Vous pouvez également personnaliser d'autres paramètres ARP. Vous pouvez personnaliser le tableau d'adresses MAC pour les groupes de ponts, y compris en ajoutant une entrée ARP statique pour éviter l'usurpation d'adresse MAC.

Inspection ARP pour le trafic de groupe de ponts

Par défaut, tous les paquets ARP sont autorisés entre les membres du groupe de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP.

L'inspection ARP empêche les utilisateurs malveillants d'usurper l'identité d'autres hôtes ou routeurs (connue sous le nom d'usurpation d'identité ARP). L'usurpation d'identité ARP peut permettre une attaque de l'intercepteur. Par exemple, un hôte envoie une requête ARP au routeur de passerelle; le routeur de passerelle répond par l'adresse MAC du routeur de passerelle. Cependant, l'agresseur envoie une autre réponse ARP à l'hôte avec l'adresse MAC de l'agresseur au lieu de l'adresse MAC du routeur. L'agresseur peut désormais intercepter tout le trafic de l'hôte avant de le transférer au routeur.

L'inspection ARP garantit qu'un agresseur ne peut pas envoyer une réponse ARP avec l'adresse MAC de l'agresseur, tant que la bonne adresse MAC et l'adresse IP associée figurent dans le tableau ARP statique.

Lorsque vous activez l'inspection ARP, ASA compare l'adresse MAC, l'adresse IP et l'interface source de tous les paquets ARP aux entrées statiques du tableau ARP, et effectue les actions suivantes :

- Si l’adresse IP, l’adresse MAC et l’interface source correspondent à une entrée ARP, le paquet est transmis.
- En cas de non-concordance entre l’adresse MAC, l’adresse IP ou l’interface, ASA abandonne le paquet.
- Si le paquet ARP ne correspond à aucune entrée dans le tableau ARP statique, vous pouvez définir ASA pour transférer le paquet hors de toutes les interfaces (flood) (submersion), ou pour abandonner le paquet.

Remarque L’interface dédiée Management (gestion) ne submerge jamais de paquets, même si ce paramètre est réglé à flood.

Tableau d'adresses MAC

Lorsque vous utilisez des groupes de ponts, l’ASA apprend et construit un tableau d’adresses MAC de la même manière qu’un pont ou un commutateur normal : lorsqu’un périphérique envoie un paquet par l’intermédiaire du groupe de ponts, l’ASA ajoute l’adresse MAC à son tableau. Le tableau associe l’adresse MAC à l’interface source de sorte que l’ASA sache envoyer tous les paquets adressés au périphérique par la bonne interface. Comme le trafic entre les membres du groupe de ponts est soumis à la politique de sécurité ASA, si l’adresse MAC de destination d’un paquet ne figure pas dans le tableau, l’ASA ne submerge pas le paquet d’origine sur toutes les interfaces comme un pont normal le fait. Au lieu de cela, il génère les paquets suivants pour les périphériques connectés directement ou pour les périphériques distants :

- Paquets pour les périphériques connectés directement : l’ASA génère une requête ARP pour l’adresse IP de destination, afin de pouvoir apprendre quelle interface reçoit la réponse ARP.
- Paquets pour les périphériques distants : l’ASA génère un message ping vers l’adresse IP de destination afin de pouvoir apprendre quelle interface reçoit la réponse ping.

Le paquet d'origine est abandonné.

Pour le mode routé, vous pouvez éventuellement activer la submersion des paquets non IP sur toutes les interfaces.

Paramètres d'usine

- Si vous activez l’inspection ARP, le paramètre par défaut est d’inonder les paquets non correspondants.
- La valeur du délai d’expiration par défaut pour les entrées du tableau d’adresses MAC dynamiques est de 5 minutes.
- Par défaut, chaque interface apprend automatiquement les adresses MAC du trafic d’entrée et ASA ajoute les entrées correspondantes au tableau d’adresses MAC.

Remarque Cisco Secure Firewall ASA génère un paquet de réinitialisation pour réinitialiser une connexion qui est refusée par un moteur d'inspection dynamique. Ici, l'adresse MAC de destination du paquet n'est pas déterminée en fonction de la recherche de la table ARP, mais est plutôt tirée directement des paquets (connexions) qui sont refusés.

Lignes directrices pour l'inspection ARP et la table d'adresses MAC

- L'inspection ARP n'est possible que pour les groupes de ponts.
- La configuration de la table des adresses MAC n'est possible que pour les groupes de ponts.

Configurer l'inspection ARP et les autres paramètres ARP

Pour les groupes de ponts, vous pouvez activer l'inspection ARP. Vous pouvez également configurer d'autres paramètres ARP pour les groupes de ponts et pour les interfaces en mode routé.

Procédure

Étape 1 Ajoutez des entrées ARP statiques en fonction de Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP, à la page 927. L'inspection ARP compare les paquets ARP avec les entrées ARP statiques dans le tableau ARP. Par conséquent, des entrées ARP statiques sont nécessaires pour cette fonctionnalité. Vous pouvez également configurer d'autres paramètres ARP.

Étape 2 Activez l'inspection ARP conformément à Activer l'inspection ARP, à la page 929.

Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP

Par défaut, pour les groupes de ponts, tous les paquets ARP sont autorisés entre les interfaces membres des groupes de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP. L'inspection ARP compare les paquets ARP avec les entrées ARP *statiques* dans le tableau ARP.

Pour les interfaces routées, vous pouvez saisir des entrées ARP statiques, mais normalement, les entrées dynamiques sont suffisantes. Pour les interfaces routées, la table ARP est utilisée pour acheminer des paquets aux hôtes connectés directement. Bien que les expéditeurs identifient la destination d'un paquet par une adresse IP, la livraison réelle du paquet sur Ethernet dépend de l'adresse MAC Ethernet. Lorsqu'un routeur ou un hôte souhaite acheminer un paquet sur un réseau directement connecté, il envoie une requête ARP demandant l'adresse MAC associée à l'adresse IP, puis achemine le paquet à l'adresse MAC en fonction de la réponse ARP. L'hôte ou le routeur conserve une table ARP pour ne pas avoir à envoyer des demandes ARP pour chaque paquet à livrer. La table ARP est mise à jour dynamiquement chaque fois que des réponses ARP sont

envoyées sur le réseau et, si une entrée n'est pas utilisée pendant un certain temps, elle expire. Si une entrée est incorrecte (par exemple, l'adresse MAC change pour une adresse IP donnée), l'entrée doit expirer avant de pouvoir être mise à jour avec les nouvelles informations.

En mode transparent, l'ASA utilise uniquement les entrées ARP dynamiques de la table ARP pour le trafic entrant et sortant de l'ASA, tel que le trafic de gestion.

Vous pouvez également définir le délai d'expiration d'ARP et d'autres comportements d'ARP.

Procédure

Étape 1 Ajoutez une entrée ARP statique :

arp *interface_name ip_address mac_address* [**alias**]

Exemple :

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Cet exemple autorise les réponses ARP du routeur à l'adresse 10.1.1.1 avec l'adresse MAC 0009.7cbe.2100 sur l'interface externe.

Précisez **alias** dans le mode routé pour activer le serveur mandataire ARP pour ce mappage. Si l'ASA reçoit une requête ARP pour l'adresse IP spécifiée, il répond par l'adresse MAC de l'ASA. Ce mot clé est utile si certains de vos périphériques n'effectuent pas d'ARP, par exemple. En mode transparent de pare-feu, ce mot clé est ignoré; l'ASA n'exécute pas le protocole ARP par mandataire.

Étape 2 Définissez le délai d'expiration ARP pour les entrées ARP dynamiques :

arp timeout *secondes*

Exemple :

```
ciscoasa(config)# arp timeout 5000
```

Ce champ définit le délai avant que l'ASA recrée la table ARP, entre 60 et 4294967 secondes. La valeur par défaut est de 14400 secondes. La reconstitution de la table ARP met automatiquement à jour les nouvelles informations sur l'hôte et supprime les anciennes. Vous pourriez souhaiter réduire le délai d'expiration, car les informations sur l'hôte changent fréquemment.

Étape 3 Autorisez les sous-réseaux non connectés :

arp permit-nonconnected

Le cache ARP de l'ASA contient uniquement les entrées des sous-réseaux connectés directement par défaut. Vous pouvez activer le cache ARP pour inclure également les sous-réseaux non connectés directement. Nous vous déconseillons d'activer cette fonctionnalité, sauf si vous connaissez les risques de sécurité. Cette fonctionnalité pourrait faciliter les attaques par déni de service contre l'ASA; un utilisateur, sur n'importe quelle interface, pourrait envoyer de nombreuses réponses ARP et sur téléverser la table ARP de l'ASA de fausses entrées.

Vous souhaiterez peut-être utiliser cette fonctionnalité si vous utilisez :

- Sous-réseaux secondaires.

- Serveur mandataire ARP sur les routes adjacentes pour le transfert du trafic.

Étape 4 Définissez la limite de débit ARP pour contrôler le nombre de paquets ARP par seconde :

arp rate-limit *secondes*

Exemple :

```
ciscoasa(config)# arp rate-limit 1000
```

Saisissez une valeur entre 10 et 32 768. La valeur par défaut dépend de votre modèle d'ASA. Vous pouvez personnaliser cette valeur pour empêcher une attaque de tempête ARP.

Activer l'inspection ARP

Cette section décrit comment activer l'inspection ARP pour les groupes de ponts.

Procédure

Activez l'inspection ARP :

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

Exemple :

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

Le mot clé **flood** transfère les paquets ARP non correspondants sur toutes les interfaces et **no-flood** abandonne les paquets non correspondants.

Le paramètre par défaut est d'inonder les paquets non correspondants. Pour restreindre le protocole ARP par l'ASA aux entrées statiques uniquement, définissez cette commande sur **no-flood**.

Personnaliser la table des adresses MAC pour les groupes de ponts

Cette section décrit comment vous pouvez personnaliser le tableau d'adresses MAC pour les groupes de ponts.

Ajouter une adresse MAC statique pour les groupes de ponts

Normalement, les adresses MAC sont ajoutées au tableau d'adresses MAC de manière dynamique au fur et à mesure que le trafic en provenance d'une adresse MAC particulière entre dans une interface. Vous pouvez ajouter des adresses MAC statiques au tableau d'adresses MAC. L'ajout d'entrées statiques offre l'avantage de prévenir l'usurpation d'adresse MAC. Si un client avec la même adresse MAC qu'une entrée statique tente

d'envoyer le trafic vers une interface qui ne correspond pas à l'entrée statique, l'ASA abandonne le trafic et génère un message système. Lorsque vous ajoutez une entrée ARP statique (voir Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP, à la page 927), une entrée d'adresse MAC statique est automatiquement ajoutée au tableau d'adresses MAC.

Pour ajouter une adresse MAC statique au tableau d'adresses MAC, procédez comme suit.

Procédure

Ajouter une adresse MAC statique

mac-address-table statique *interface_name mac_address*

Exemple :

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

Le *nom d'interface* est l'interface source.

Définir le délai d'expiration de l'adresse MAC

La valeur du délai d'expiration par défaut pour les entrées du tableau d'adresses MAC dynamiques est de 5 minutes, mais vous pouvez modifier ce délai. Pour modifier le délai d'expiration, procédez comme suit.

Procédure

Définissez le délai d'expiration de l'entrée d'adresse MAC :

mac-address-table aging-time *timeout_value*

Exemple :

```
ciscoasa(config)# mac-address-table aging-time 10
```

La valeur *timeout_value* (en minutes) est comprise entre 5 et 720 (12 heures). La valeur par défaut est de 5 minutes.

Configurer l'apprentissage de l'adresse MAC

Par défaut, chaque interface apprend automatiquement les adresses MAC du trafic d'entrée et l'ASA ajoute les entrées correspondantes au tableau d'adresses MAC. Vous pouvez désactiver l'apprentissage des adresses MAC si vous le souhaitez; cependant, à moins que vous ajoutiez statiquement des adresses MAC au tableau, aucun trafic ne peut passer par l'ASA. En mode routé, vous pouvez activer la submersion des paquets non IP sur toutes les interfaces.

Pour configurer l'apprentissage des adresses MAC, procédez comme suit :

Procédure

Étape 1 Désactivez l'apprentissage des adresses MAC :

mac-learn *interface_name* **disable**

Exemple :

```
ciscoasa(config)# mac-learn inside disable
```

La forme **no** (non) de cette commande réactive l'apprentissage des adresses MAC.

La commande **clear configure mac-learn** réactive l'apprentissage des adresses MAC sur toutes les interfaces.

Étape 2 (Mode routé uniquement) Activez la submersion des paquets non IP.

mac-learn flood

Exemple :

```
ciscoasa(config)# mac-learn flood
```

Supervision de l'inspection ARP et de la table des adresses MAC

- **show arp-inspection**

  Supervise l'inspection ARP. Affiche les paramètres actuels pour l'inspection ARP sur toutes les interfaces.

- **show mac-address-table [*interface_name*]**

  Supervise le tableau d'adresses MAC. Vous pouvez afficher le tableau d'adresses MAC entier (y compris les entrées statiques et dynamiques pour les deux interfaces) ou vous pouvez afficher le tableau d'adresses MAC d'une interface.

  Voici un exemple de sortie de la commande **show mac-address-table** qui affiche le tableau entier :

```
ciscoasa# show mac-address-table
interface        mac address           type         Time Left
------------------------------------------------------------------------
outside     0009.7cbe.2100       static    -
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

  Voici un exemple de sortie de la commande **show mac-address-table** qui affiche le tableau de l'interface interne :

```
ciscoasa# show mac-address-table inside
```

```
interface        mac address       type         Time Left
------------------------------------------------------------------------
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

Voici un exemple de sortie de la commande **show mac-address-table** qui affiche le nombre total d'entrées de groupe de ponts statiques et dynamiques :

```
ciscoasa# show mac-address-table count
Static     mac-address bridges (curr/max): 0/16384
Dynamic    mac-address bridges (curr/max): 0/16384
```

Historique de l'inspection ARP et de la table des adresses MAC

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Inspection ARP	7.0(1)	L'inspection ARP compare l'adresse MAC, l'adresse IP et l'interface source de tous les paquets ARP aux entrées statiques du tableau ARP. Cette fonctionnalité est disponible pour le mode de pare-feu transparent et pour les interfaces d'un groupe de ponts en mode transparent et en mode routé à partir de la version 9.7(1). Nous avons introduit les commandes suivantes : **arp**, **arp-inspection** et **show arp-inspection**.
Tableau d'adresses MAC	7.0(1)	Vous souhaiterez peut-être personnaliser le tableau des adresses MAC pour le mode transparent et pour les interfaces d'un groupe de ponts en mode transparent et en mode routé à partir de la version 9.7(1). Nous avons introduit les commandes suivantes : **mac-address-table static**, **mac-address-table aging-time**, **mac-learn disable** et **show mac-address-table**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Ajouts de cache ARP pour les sous-réseaux non connectés	8.4(5)/9.1(2)	Le cache ARP de l'ASA contient uniquement les entrées des sous-réseaux connectés directement par défaut. Vous pouvez désormais activer le cache ARP pour inclure également les sous-réseaux non connectés directement. Nous vous déconseillons d'activer cette fonctionnalité, sauf si vous connaissez les risques de sécurité. Cette fonctionnalité pourrait faciliter les attaques par déni de service contre l'ASA; un utilisateur, sur n'importe quelle interface, pourrait envoyer de nombreuses réponses ARP et sur téléverser la table ARP de l'ASA de fausses entrées. Vous souhaiterez peut-être utiliser cette fonctionnalité si vous utilisez : • Sous-réseaux secondaires. • Serveur mandataire ARP sur les routes adjacentes pour le transfert du trafic. Nous avons introduit la commande suivante : **arp permit-nonconnected**.
Limitation de débit ARP personnalisable	9.6(2)	Vous pouvez définir le nombre maximum de paquets ARP autorisés par seconde. La valeur par défaut dépend de votre modèle d'ASA. Vous pouvez personnaliser cette valeur pour empêcher une attaque de tempête ARP. Nous avons ajouté les commandes suivantes : **arp rate-limit, show arp rate-limit**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage et pont intégrés	9.7(1)	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que l'ASA relie par des ponts au lieu de routes. L'ASA n'est pas un vrai pont, car l'ASA continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur l'ASA à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : mode de contexte multiple, mise en grappe d'ASA. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Nous avons modifié les commandes suivantes : **access-group, access-list ethertype, arp-inspection, dhcpd, mac-address-table static, mac-address-table aging-time, mac-learn, route, show arp-inspection, show bridge-group, show mac-address-table, show mac-learn**



PARTIE V

Routage IP

- Aperçu du routage, à la page 937
- Routages statiques et par défaut, à la page 951
- Routage basé sur une stratégie, à la page 961
- Cartes de routage, à la page 981
- Routage par détection de transfert bidirectionnel (BFD), à la page 989
- BGP, à la page 999
- OSPF, à la page 1041
- IS-IS, à la page 1105
- EIGRP, à la page 1157
- Routage multidiffusion, à la page 1181



CHAPITRE 27

Aperçu du routage

Ce chapitre décrit le comportement du routage dans l'ASA.

- Détermination du chemin, à la page 937
- Types de routage pris en charge, à la page 938
- Protocoles Internet pris en charge pour le routage, à la page 939
- Table de routage, à la page 940
- Table de routage pour le trafic de gestion, à la page 947
- Routage à chemins multiples à coûts égaux (ECMP), à la page 948
- Désactiver les demandes ARP du mandataire, à la page 949
- Afficher la table de routage, à la page 949
- Historique de l'aperçu du routage, à la page 950

Détermination du chemin

Les protocoles de routage utilisent des métriques pour évaluer quel chemin sera le meilleur à parcourir pour un paquet. Une métrique est une norme de mesure, telle que la bande passante du chemin, utilisée par les algorithmes de routage pour déterminer le chemin optimale vers une destination. Pour faciliter le processus de détermination du chemin, les algorithmes de routage lancent et gèrent les tableaux de routage, qui comprennent les informations de routage. Les informations de route varient en fonction de l'algorithme de routage utilisé.

Les algorithmes de routage remplissent les tableaux de routage avec diverses informations. Les associations de destination ou du prochain saut indiquent à un routeur qu'une destination particulière peut être atteinte de manière optimale en envoyant le paquet à un routeur particulier représentant le prochain saut sur le chemin vers la destination finale. Lorsqu'un routeur reçoit un paquet entrant, il vérifie l'adresse de destination et tente d'associer cette adresse à un saut suivant.

Les tableaux de routage peuvent également comprendre d'autres informations, telles que des données sur l'opportunité d'un chemin. Les routeurs comparent les métriques pour déterminer les routes optimales. Ces métriques varient en fonction de la conception de l'algorithme de routage utilisé.

Les routeurs communiquent entre eux et gèrent leurs tables de routage par la transmission de divers messages. Le message de mise à jour du routage en est un qui consiste généralement en tout ou en partie d'une table de routage. En analysant les mises à jour de routage de tous les autres routeurs, votre routeur peut dresser un tableau détaillé de la topologie du réseau. Une annonce d'état de lien, un autre exemple de message envoyé entre des routeurs, informe les autres routeurs de l'état des liens de l'expéditeur. Les informations sur la liaison

peuvent également être utilisées pour dresser une image complète de la topologie du réseau afin de permettre aux routeurs de déterminer les routes optimales vers les destinations du réseau.

Remarque Le routage symétrique est uniquement pris en charge pour le basculement actif/actif dans le mode de contexte multiple.

Types de routage pris en charge

Un routeur peut utiliser plusieurs types de routage. L'ASA utilise les types de routage suivants :

- Statique ou dynamique
- Chemin unique ou chemin multiple
- Non hiérarchique ou hiérarchique
- État de lien ou vecteur de distance

Statique ou dynamique

Les algorithmes de routage statique sont en fait des mappages de tables établis par l'administrateur réseau. Ces mappages ne changent pas, sauf si l'administrateur réseau les modifie. Les algorithmes qui utilisent des routes statiques sont simples à concevoir et fonctionnent bien dans des environnements où le trafic réseau est relativement fiable et où la conception de réseau est relativement simple.

Étant donné que les systèmes de routage statique ne peuvent pas réagir aux modifications du réseau, ils sont généralement considérés comme ne convenant pas aux grands réseaux en constante évolution. La plupart des algorithmes de routage prédominants sont des algorithmes de routage dynamique, qui s'adaptent aux circonstances changeantes du réseau en analysant les messages de mise à jour de routage entrants. Si le message indique qu'un changement de réseau est survenu, le logiciel de routage recalcule les routages et envoie de nouveaux messages de mise à jour de routage. Ces messages pénètrent dans le réseau, incitant les routeurs à réexécuter leurs algorithmes et à modifier leurs tables de routage en conséquence.

Les algorithmes de routage dynamique peuvent être complétés par des routes statiques, le cas échéant. Un routeur de dernier recours (une voie de routage par défaut pour un routeur auquel tous les paquets non routables sont envoyés), par exemple, peut être désigné pour servir de référentiel pour tous les paquets non routables, garantissant que tous les messages sont au moins gérés d'une manière ou d'une autre.

Chemin unique ou chemin multiple

Certains protocoles de routage sophistiqués prennent en charge plusieurs chemins vers la même destination. Contrairement aux algorithmes à chemin unique, ces algorithmes à chemins multiples permettent le multiplexage du trafic sur plusieurs lignes. Les avantages des algorithmes par chemins multiples sont un débit et une fiabilité considérablement meilleurs, ce qui est généralement appelé partage de charge.

Non hiérarchique ou hiérarchique

Certains algorithmes de routage fonctionnent dans un espace à plat, tandis que d'autres utilisent des hiérarchies de routage. Dans un système de routage à plat, les routeurs sont les homologues de tous les autres. Dans un système de routage hiérarchique, certains routeurs forment ce qui équivaut à un réseau fédérateur (backbone) de routage. Les paquets provenant de routeurs ne faisant pas partie du réseau fédérateur sont acheminés vers les routeurs de ce dernier, où ils sont envoyés à travers le réseau fédérateur jusqu'à ce qu'ils atteignent la zone générale de la destination.. À ce stade, ils se déplacent du dernier routeur de réseau fédérateur à un ou plusieurs routeurs hors du réseau fédérateur jusqu'à la destination finale.

Les systèmes de routage désignent souvent des groupes logiques de nœuds, appelés domaines, systèmes autonomes ou zones. Dans les systèmes hiérarchiques, certains routeurs d'un domaine peuvent communiquer avec les routeurs d'autres domaines, tandis que d'autres ne peuvent communiquer qu'avec les routeurs de leur domaine. Dans les très grands réseaux, il peut exister des niveaux hiérarchiques supplémentaires, les routeurs du niveau hiérarchique le plus élevé constituant le réseau fédérateur de routage.

Le principal avantage du routage hiérarchique est qu'il imite l'organisation de la plupart des entreprises et, par conséquent, prend bien en charge leurs schémas de trafic. La plupart des communications réseau se produisent au sein de petits groupes d'entreprise (domaines). Comme les routeurs intra-domaines n'ont besoin de connaître que les autres routeurs de leur domaine, leurs algorithmes de routage peuvent être simplifiés et, selon l'algorithme de routage utilisé, le trafic de mise à jour de routage peut être réduit en conséquence.

État de lien ou vecteur de distance

Les algorithmes d'état de liens (également appelés algorithmes du plus court chemin d'abord) acheminent les informations de routage à tous les nœuds de l'inter-réseau. Cependant, chaque routeur envoie uniquement la partie de la table de routage qui décrit l'état de ses propres liaisons. Dans les algorithmes à état de liens, chaque routeur construit une image de l'ensemble du réseau dans ses tables de routage. Les algorithmes de vecteurs de distance (également appelés algorithmes de Bellman-Ford) exigent que chaque routeur envoie la totalité ou une partie de sa table de routage, mais uniquement à ses voisins. En gros, les algorithmes à état de liens envoient de petites mises à jour partout, tandis que les algorithmes à vecteur de distance envoient des mises à jour plus volumineuses uniquement aux routeurs voisins. Les algorithmes de vecteurs de distance ne connaissent que leurs voisins. En règle générale, les algorithmes d'état de liaison sont utilisés conjointement avec les protocoles de routage OSPF.

Protocoles Internet pris en charge pour le routage

L'ASA prend en charge plusieurs protocoles Internet pour le routage. Chaque protocole est décrit brièvement dans cette section.

- Protocole de routage de passerelle intérieure amélioré (EIGRP)

  EIGRP est un protocole exclusif de Cisco qui assure la compatibilité et une interopération transparente avec les routeurs IGRP. Un mécanisme de redistribution automatique permet aux routes IGRP d'être importées dans le protocole Enhanced IGRP, et inversement. Il est donc possible d'ajouter progressive-ment le protocole Enhanced IGRP à un réseau IGRP existant.

- Open Shortest Path First (OSPF)

  OSPF est un protocole de routage mis au point pour les réseaux IP (Internet Protocol) par le groupe de travail IGP (Interior Gateway Protocol) de l'Internet Engineering Task Force (IETF). OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues.

Chaque routeur d'une zone OSPF comprend une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

- Protocole RIP (Routing Information Protocol)

  IPS est un protocole de vecteur de distance qui utilise le nombre de sauts comme mesure. Il s'agit d'un protocole IGP (Interior Gateway Protocol), ce qui signifie qu'il effectue le routage au sein d'un seul système autonome.

- Protocole de routage BGP

  BGP est un protocole de routage de système inter autonome. BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les fournisseurs de services Internet (ISP). Les clients se connectent aux fournisseurs de services Internet, et les fournisseurs de services Internet utilisent BGP pour échanger les routes du client et des fournisseurs de services Internet. Lorsque BGP est utilisé entre des systèmes autonomes (AS), le protocole est appelé BGP externe (EBGP). Si un fournisseur de services utilise BGP pour échanger des routages au sein d'un système autonome, le protocole est appelé BGP intérieur (IBGP).

- Intermediate System-to-Intermediate System (IS-IS)

  IS-IS est un protocole IGP (Interior Gateway Protocol) à état de liaison. Les protocoles à état de liaison se caractérisent par la propagation des informations nécessaires pour créer une carte complète de la connectivité du réseau sur chaque routeur participant. Cette carte est ensuite utilisée pour calculer le chemin le plus court vers les destinations.

Table de routage

Le ASA utilise des tableaux de routage distincts pour le trafic de données (via le périphérique) et pour le trafic de gestion (du périphérique). Cette section décrit le fonctionnement des tables de routage. Pour en savoir plus sur la table de routage de gestion, consultez également Table de routage pour le trafic de gestion, à la page 947.

Mode de remplissage de la table de routage

La table de routage ASA peut être remplie par des routes définies de manière statique, des routes connectées directement et des routes découvertes par les protocoles de routage dynamique. Comme le périphérique ASA peut exécuter plusieurs protocoles de routage en plus d'avoir des routes statiques et connectées dans la table de routage, il est possible qu'une même route soit découverte ou saisie de plusieurs manières. Lorsque deux routes vers la même destination sont mises dans la table de routage, celle qui reste dans la table de routage est déterminée comme suit :

- Si les deux routes ont des longueurs de préfixe de réseau différentes (masques de réseau), les deux routes sont considérées comme uniques et sont entrées dans la table de routage. La logique de transfert de paquets détermine ensuite laquelle des deux utiliser.

  Par exemple, si les processus RIP et OSPF ont découvert les routes suivantes :

  - RIP : 192.168.32.0/24
  - OSPF : 192.168.32.0/19

Même si les routes OSPF ont la meilleure distance administrative, les deux routes sont installées dans la table de routage, car chacune de ces routes a une longueur de préfixe différente (masque de sous-réseau). Ce sont des destinations considérées comme différentes et la logique de transfert de paquets détermine la route à utiliser.

- Si le périphérique ASA connaît plusieurs chemins vers la même destination à partir d'un protocole de routage unique, comme RIP, la voie de routage avec la meilleure mesure (déterminée par le protocole de routage) est entrée dans la table de routage.

  Les métriques sont des valeurs associées à des routes spécifiques, de la plus préférée à la moins préférée. Les paramètres utilisés pour déterminer les métriques varient selon le protocole de routage. Le chemin avec la mesure la plus basse est sélectionné comme chemin optimale et installé dans la table de routage. S'il existe plusieurs chemins vers la même destination avec des métriques égales, l'équilibrage de la charge est effectué sur ces chemins de coût égal.

- Si le périphérique ASA connaît une destination à partir de plus d'un protocole de routage, les distance administratives des routages sont comparées et les routes avec une distance administrative inférieure sont entrées dans la table de routage.

Distances administratives pour les routages

Vous pouvez modifier les distance administratives pour les routages détectés ou redistribués dans un protocole de routage. Si deux routes de deux protocoles de routage différents ont la même distance administrative, la route avec la distance administrative *par défaut* la plus faible est entrée dans la table de routage. Dans le cas des routes EIGRP et OSPF, si la route EIGRP et la route OSPF ont la même distance administrative, la route EIGRP est choisie par défaut.

La distance administrative est un paramètre de routage que ASA utilise pour sélectionner le meilleur chemin lorsqu'il existe deux ou plusieurs itinéraires différents vers la même destination à partir de deux protocoles de routage différents. Puisque les protocoles de routage ont des mesures basées sur des algorithmes différents des autres protocoles, il n'est pas toujours possible de déterminer le meilleur chemin pour deux routages vers la même destination qui ont été générées par différents protocoles de routage.

Chaque protocole de routage est priorisé à l'aide d'une valeur de distance administrative. Le tableau suivant présente les valeurs de distance administrative par défaut pour les protocoles de routage pris en charge par ASA.

Tableau 34 : Distance administrative par défaut pour les protocoles de routage pris en charge

Source de la route	Distance administrative par défaut
Interface connectée	0
Routage VPN	1
Routage statique	1
Routage résumé EIGRP	5
BGP externe	20
EIGRP interne	90
OSPF	110

Source de la route	Distance administrative par défaut
IS-IS	115
RIP	120
Routage EIGRP externe	170
BGP interne et local	200
Inconnu	255

Plus la valeur de la distance administrative est faible, plus la préférence est donnée au protocole. Par exemple, si l'ASA reçoit une voie de routage vers un certain réseau d'un processus de routage OSPF (distance administrative par défaut - 110) et d'un processus de routage RIP (distance administrative par défaut - 120), l'ASA choisit la voie de routage OSPF, car OSPF a une préférence plus élevée. Dans ce cas, le routeur ajoute la version OSPF de la route à la table de routage.

Une route VPN annoncée (V-Route/RRI) équivaut à une route statique avec la distance administrative par défaut de 1. Mais elle comporte une préférence plus élevée, comme avec le masque de réseau 255.255.255.255.

Dans cet exemple, si la source de routage dérivée OSPF était perdue (par exemple, en raison d'une coupure de courant), l'ASA utiliserait alors le routage dérivé RIP jusqu'à ce que le routage dérivé OSPF réapparaisse.

La distance administrative est un paramètre local. Par exemple, si vous modifiez la distance administrative des routages obtenus par OSPF, cette modification n'affectera que la table de routage du ASA pour lequel la commande a été saisie. La distance administrative n'est pas annoncée dans les mises à jour de routage.

La distance administrative n'affecte pas le processus de routage. Les processus de routage n'annoncent que les routages détectés par le processus de routage ou redistribués dans le processus de routage. Par exemple, le processus de routage RIP annonce les routes RIP, même si les routes découvertes par le processus de routage OSPF sont utilisées dans la table de routage.

Sauvegarde des routes dynamiques et statiques flottantes

Une route de secours est enregistrée lorsque la tentative initiale d'installation de la route dans la table de routage échoue parce qu'une autre route a été installée à la place. Si la voie de routage qui a été installée dans la table de routage échoue, le processus de maintenance de la table de routage appelle chaque processus de protocole de routage qui a enregistré une voie de routage de secours et lui demande de réinstaller la voie de routage dans la table de routage. S'il existe plusieurs protocoles avec des routes de secours enregistrées pour la voie de routage ayant échoué, la voie de routage préférée est choisie en fonction de la distance administrative.

Grâce à ce processus, vous pouvez créer des routes statiques flottantes qui sont installées dans la table de routage lorsque la route découverte par un protocole de routage dynamique échoue. Une voie de routage statique flottante est tout simplement une voie de routage statique configurée avec une distance administrative supérieure à celle des protocoles de routage dynamique s'exécutant sur ASA. Lorsque la voie de routage correspondante découverte par un processus de routage dynamique échoue, la voie de routage statique est installée dans la table de routage.

Prise des décisions de transfert

Les décisions de transfert sont prises comme suit :

- Si la destination ne correspond à aucune entrée de la table de routage, le paquet est acheminé par l'intermédiaire de l'interface spécifiée pour la voie de routage par défaut. Si une voie de routage par défaut n'a pas été configurée, le paquet est rejeté.
- Si la destination correspond à une seule entrée dans la table de routage, le paquet est acheminé par l'interface associée à cette voie de routage.
- Si la destination correspond à plus d'une entrée dans la table de routage, le paquet est transféré hors de l'interface associée à la voie de routage qui a la plus grande longueur de préfixe de réseau.

Par exemple, un paquet destiné à 192.168.32.1 arrive sur une interface avec les routes suivantes dans la table de routage :

- Passerelle 192.168.32.0/24 10.1.1.2
- Passerelle 192.168.32.0/19 10.1.1.3

Dans ce cas, un paquet destiné à 192.168.32.1 est dirigé vers 10.1.1.2, car 192.168.32.1 fait partie du réseau 192.168.32.0/24. Il fait également partie de l'autre voie de routage dans la table de routage, mais 192.168.32.0/24 a le préfixe le plus long dans la table de routage (24 bits vers 19 bits). Les préfixes les plus longs sont toujours préférables aux plus courts lors du transfert d'un paquet.



Remarque Les connexions existantes continuent d'utiliser leurs interfaces établies même si une nouvelle connexion similaire entraînerait un comportement différent en raison d'une modification des routages.

Routage dynamique et Failover (basculement)

Les routages dynamiques sont synchronisés sur l'unité de secours lorsque la table de routage change sur l'unité active. Cela signifie que tous les ajouts, suppressions ou modifications effectués sur l'unité active sont immédiatement répercutés sur l'unité en veille. Si l'unité de secours devient active dans une paire actif/secours Failover (basculement) prête, elle aura déjà une table de routage identique à celle de l'unité active précédente, car les routages sont synchronisés dans le cadre de la synchronisation en bloc Failover (basculement) et des processus de duplication continue.

Routage et mise en grappe dynamiques

Cette section décrit comment utiliser le routage dynamique avec la mise en grappe.

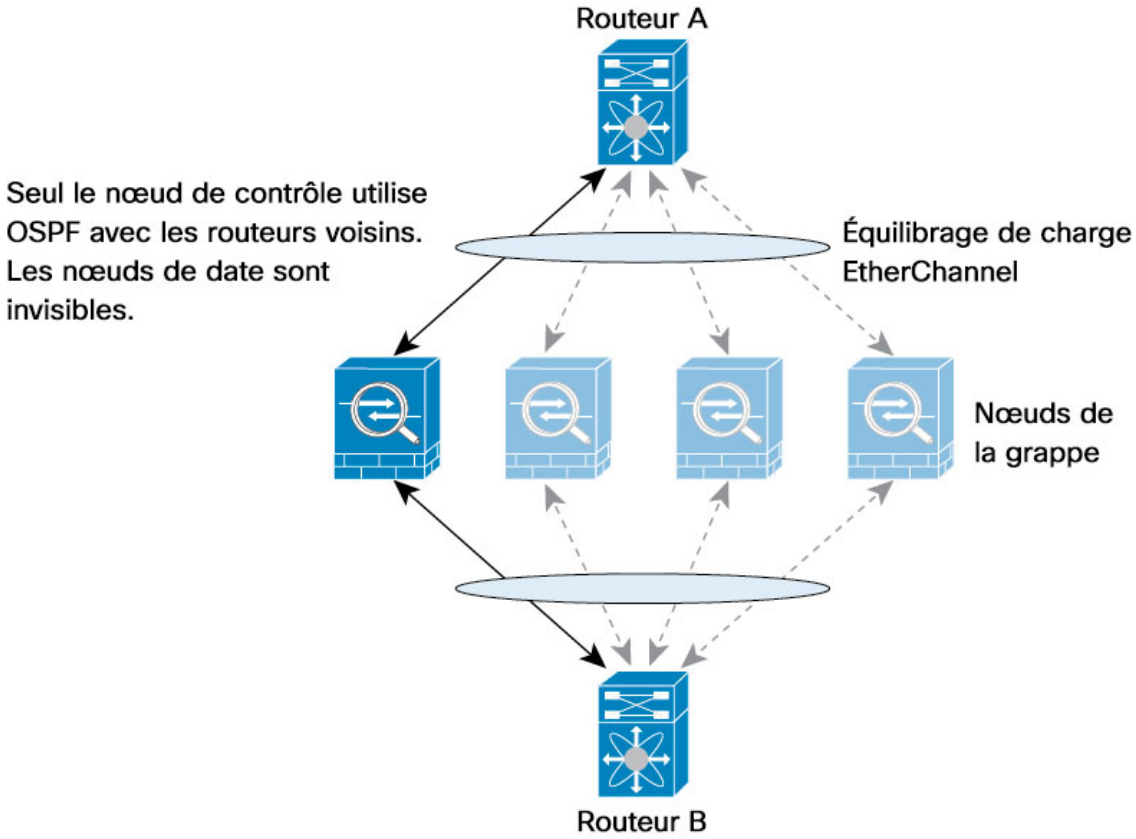
Routage dynamique en mode EtherChannel étendu



Remarque IS-IS n'est pas pris en charge en mode EtherChannel étendu.

Le processus de routage ne s'exécute que sur le nœud de contrôle, et les routes sont apprises par le nœud de contrôle et répliquées sur les nœuds de données. Si un paquet de routage arrive à un nœud de données, il est redirigé vers le nœud de contrôle.

Illustration 66 : Routage dynamique en mode EtherChannel étendu



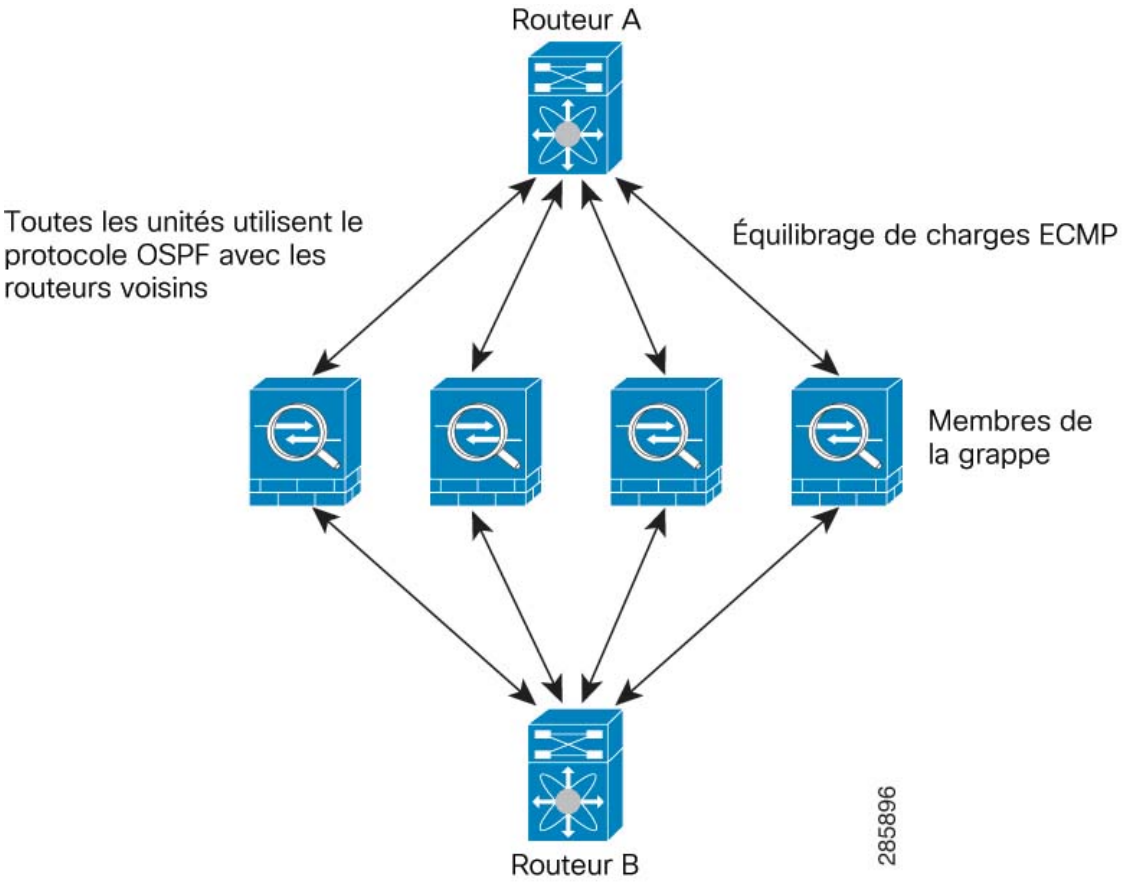
Une fois que le nœud de données a appris les routes du nœud de contrôle, chaque nœud prend des décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée du nœud de contrôle avec les nœuds de données. S'il y a basculement du nœud de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

Routage dynamique en mode d'interface individuelle

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 67 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Remarque Si la grappe comporte plusieurs contiguïtés avec le même routeur à des fins de redondance, le routage dissymétrique peut entraîner une perte de trafic inacceptable. Pour éviter le routage dissymétrique, regroupez toutes ces interfaces de nœud dans la même zone de trafic. Voir Configurer une zone de trafic, à la page 822.

Routage dynamique en mode de contexte multiple

En mode de contexte multiple, chaque contexte gère une table de routage et des bases de données de protocole de routage distinctes. Cela vous permet de configurer les protocoles OSPFv2 et EIGRP indépendamment dans chaque contexte. Vous pouvez configurer le protocole EIGRP dans certains contextes et le protocole OSPFv2

dans le même contexte ou des contextes différents. En mode de contexte mixte, vous pouvez activer n'importe quel protocole de routage dynamique dans les contextes qui sont en mode routé. Les protocoles RIP et OSPFv3 ne sont pas pris en charge en mode de contexte multiple.

Le tableau suivant répertorie les attributs des protocoles EIGRP et OSPFv2, les cartes de routage utilisées pour la distribution des routes dans les processus OSPFv2 et EIGRP, ainsi que les listes de préfixes utilisées dans le protocole OSPFv2 pour filtrer les mises à jour de routage entrant ou sortant d'une zone lorsqu'elles sont utilisées en mode de contexte multiple :

EIGRP	OSPFv2	Cartes de routage et listes de préfixes
Une instance est prise en charge par contexte.	Deux instances sont prises en charge par contexte.	S. O.
Il est désactivé dans le contexte système.		S. O.
Deux contextes peuvent utiliser les mêmes numéros de système autonome ou des numéros différents.	Deux contextes peuvent utiliser des ID de zone identiques ou différents.	S. O.
Les interfaces partagées dans deux contextes peuvent avoir plusieurs instances EIGRP en cours d'exécution.	Les interfaces partagées dans deux contextes peuvent avoir plusieurs instances OSPF en cours d'exécution.	S. O.
L'interaction des instances EIGRP sur les interfaces partagées est prise en charge.	L'interaction des instances OSPFv2 sur les interfaces partagées est prise en charge.	S. O.
Toutes les interfaces de ligne de commande disponibles en mode unique le sont également en mode de contexte multiple.		
Chaque interface de ligne de commande n'a d'effet que dans le contexte dans lequel elle est utilisée.		

Gestion des ressources de routage

Une classe de ressources appelée *routes* spécifie le nombre maximum d'entrées de table de routage pouvant exister dans un contexte. Cela résout le problème d'un contexte affectant les entrées de table de routage disponibles dans un autre contexte et vous permet également de mieux contrôler le nombre maximum d'entrées de route par contexte.

Comme il n'y a pas de limite système définitive, vous pouvez uniquement spécifier une valeur absolue pour cette limite de ressource; vous ne pouvez pas utiliser de limite de pourcentage. De plus, il n'y a pas de limites minimum et maximum par contexte, de sorte que la classe par défaut ne change pas. Si vous ajoutez une nouvelle route pour l'un des protocoles de routage statique ou dynamique (connecté, statique, OSPF, EIGRP et RIP) dans un contexte et que la limite de ressources pour ce contexte est expirée, l'ajout de route échoue et un message de journal système est généré.

Table de routage pour le trafic de gestion

En tant que pratique de sécurité courante, il est souvent nécessaire de séparer et d'isoler le trafic de gestion (provenant du périphérique) du trafic de données. Pour réaliser cet isolement, le périphérique ASA utilise une table de routage distincte pour le trafic de gestion uniquement par rapport au trafic de données. Des tableaux de routage distincts signifient que vous pouvez créer des routages par défaut distincts pour les données et la gestion.

Types de trafic pour chaque table de routage

Le trafic de l'appareil utilise toujours la table de routage des données.

Le trafic en provenance du périphérique, selon le type, utilise par défaut la table de tourage réservé à la gestion ou la table de routage des données. Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

- Le trafic de la table de gestion uniquement à partir de l'appareil comprend des fonctionnalités qui ouvrent un fichier distant à l'aide de HTTP, SCP, TFTP, la commande **copy** , les licences Smart, Smart Call Home, **trustpointtrustpool**, etc.
- Le trafic du tableau de données du périphérique comprend toutes les autres fonctionnalités telles que le ping, le DNS, le DHCP, etc.

Interfaces incluses dans la table de routage de gestion uniquement

Les interfaces de gestion uniquement comprennent toutes les interfaces x/x Management (gestion) ainsi que toutes les interfaces que vous avez configurées pour être uniquement de gestion.

Repli vers l'autre table de routage

Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

Utilisation de la table de routage autre que par défaut

Si vous avez besoin que le trafic initial sorte d'une interface qui ne figure pas dans sa table de routage par défaut, vous devrez peut-être spécifier cette interface lorsque vous la configurerez, plutôt que de vous fier à l'autre table. Le ASA vérifiera uniquement les routes pour l'interface spécifiée. Par exemple, si vous avez besoin d'un ping pour sortir une interface de gestion uniquement, spécifiez l'interface dans la fonction envoyer un message Ping. Sinon, s'il existe une route par défaut dans la table de routage de données, elle correspondra à la route par défaut et ne reviendra jamais à la table de routage de gestion.

Routage dynamique

La table de routage réservé à la gestion prend en charge le routage dynamique distinct du table de routage de l'interface de données. Un processus de routage dynamique donné doit s'exécuter sur l'interface de gestion uniquement ou sur l'interface de données; vous ne pouvez pas mélanger les deux types. Lors de la mise à niveau à partir d'une version antérieure sans table de routage de gestion distinct, si vous avez un mélange d'interfaces de données et de gestion utilisant le même processus de routage dynamique, les interfaces de gestion seront abandonnées.

Fonctionnalité d'accès de gestion pour les exigences VPN

Si vous configurez la fonctionnalité d'accès de gestion qui permet l'accès de gestion à une interface autre que celle à partir de laquelle vous avez entré l'ASA lors de l'utilisation du VPN, alors, en raison de considérations de routage avec les tables de gestion et de routage de données distinctes, l'interface de terminaison VPN et la gestion L'interface d'accès doit être du même type : les deux doivent être des interfaces de gestion uniquement ou des interfaces de données standard.

Identification de l'interface de gestion

Une interface configurée avec l'option de gestion uniquement est considérée comme une interface de gestion.

Dans la configuration suivante, les interfaces GigabitEthernet0/0 et Management0/0 sont considérées comme des interfaces de gestion.

```
a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.10.10.123 255.255.255.0
 ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#
```

Routage à chemins multiples à coûts égaux (ECMP)

L'ASA prend en charge le routage à chemins multiples à coûts égaux (ECMP).

Vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal par interface. Par exemple, vous pouvez configurer plusieurs routes par défaut sur l'interface externe qui spécifient différentes passerelles.

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

Dans ce cas, le trafic est équilibré en charge sur l'interface externe entre 10.1.1.2, 10.1.1.3 et 10.1.1.4. Le trafic est réparti entre les passerelles précisées selon un algorithme qui procède au hachage des adresses IP source et de destination, de l'interface entrante, du protocole et des ports source et destination.

ECMP sur plusieurs interfaces à l'aide de zones de trafic

Si vous configurez des zones de trafic pour contenir un groupe d'interfaces, vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal sur 8 interfaces au sein de chaque zone. Par exemple, vous pouvez configurer plusieurs routes par défaut sur trois interfaces dans la zone :

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

De même, votre protocole de routage dynamique peut configurer automatiquement des routes à coût égal. L'ASA équilibre la charge du trafic entre les interfaces grâce à un mécanisme d'équilibrage de la charge plus robuste.

Lorsqu'un routage est perdu, le périphérique déplace le flux de manière transparente vers une autre route.

Désactiver les demandes ARP du mandataire

Lorsqu'un hôte envoie du trafic IP à un autre périphérique sur le même réseau Ethernet, l'hôte doit connaître l'adresse MAC du périphérique. ARP est un protocole de couche 2 qui résout une adresse IP en une adresse MAC. Un hôte envoie une demande ARP de type « À qui appartient cette adresse IP? ». Le périphérique qui possède l'adresse IP répond : « Je possède cette adresse IP; voici mon adresse MAC. »

L'ARP du mandataire est utilisé lorsqu'un périphérique répond à une demande ARP avec sa propre adresse MAC, même si le périphérique ne possède pas l'adresse IP. L'ASA utilise un ARP de mandataire lorsque vous configurez la NAT et spécifiez une adresse mappée qui se trouve sur le même réseau que l'interface ASA. Le trafic ne peut atteindre les hôtes que si l'ASA utilise un ARP de mandataire pour revendiquer que l'adresse MAC est attribuée aux adresses mappées de destination.

Dans de rares cas, vous souhaiterez peut-être désactiver l'ARP du mandataire pour les adresses NAT.

Si vous avez un ensemble d'adresses du client VPN qui chevauche un réseau existant, l'ASA envoie par défaut des demandes ARP de mandataire sur toutes les interfaces. Si vous avez une autre interface qui se trouve sur le même domaine de couche 2, elle verra les demandes ARP et répondra par l'adresse MAC de son interface. Il en résulte que le trafic de retour des clients VPN vers les hôtes internes ira à la mauvaise interface et sera abandonné. Dans ce cas, vous devez désactiver les demandes ARP de mandataire pour l'interface sur laquelle vous ne les souhaitez pas.

Procédure

Désactivez les demandes ARP du mandataire :

sysopt noproxyarp *interface*

Exemple :

```
ciscoasa(config)# sysopt noproxyarp exampleinterface
```

Afficher la table de routage

Utilisez la commande **show route** pour afficher les entrées de la table de routage.

```
ciscoasa# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

S    10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
```

```
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

Historique de l'aperçu du routage

Tableau 35 : Historique de l'aperçu du routage

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Table de routage pour l'interface de gestion	9.5(1)	Pour séparer et isoler le trafic de gestion du trafic de données, une table de routage distincte est ajoutée pour le trafic de gestion. Des tables de routage distinctes, pour la gestion et les données respectivement, sont créées pour IPv4 et IPv6, pour chaque contexte, de l'ASA. De plus, pour chaque contexte de l'ASA, deux tables de routage supplémentaires sont ajoutées dans la RIB et la FIB. Nous avons introduit les commandes suivantes : show route management-only, show ipv6 route management-only, show asp table route-management-only, clear route management-only, clear ipv6 route management-only, copy interface <interface> tftp/ftp



CHAPITRE 28

Routages statiques et par défaut

Ce chapitre décrit comment configurer les routes statiques et par défaut sur l'ASA.

- À propos des routages statiques et par défaut, à la page 951
- Lignes directrices pour les routages statiques et par défaut, à la page 953
- Configurer les routes par défaut et statiques, à la page 954
- Supervision d'une route statique ou par défaut, à la page 958
- Exemples de routes statiques ou par défaut, à la page 959
- Historique des routes statiques et par défaut, à la page 959

À propos des routages statiques et par défaut

Pour acheminer le trafic vers un hôte ou un réseau non connecté, vous devez définir une voie de routage vers l'hôte ou le réseau, à l'aide du routage statique ou dynamique. En général, vous devez configurer au moins une route statique : une route par défaut pour tout le trafic qui n'est pas acheminé par d'autres moyens vers une passerelle de réseau par défaut, en général le routeur du saut suivant.

Routage par défaut

L'option la plus simple est de configurer une voie de routage statique par défaut pour envoyer tout le trafic vers un routeur en amont, en se fondant sur le routeur pour acheminer le trafic à votre place. Une voie de routage par défaut identifie l'adresse IP de la passerelle à laquelle ASA envoie tous les paquets IP pour lesquels il n'a pas de voie de routage statique ou apprise. Une voie de routage statique par défaut est simplement une voie de routage statique avec 0.0.0.0/0 (IPv4) ou::/0 (IPv6) comme adresse IP de destination.

Vous devez toujours définir une voie de routage par défaut.

Comme le périphérique ASA utilise des tables de routage distinctes pour le trafic de données et le trafic de gestion, vous pouvez éventuellement configurer une voie de routage par défaut pour le trafic de données et une autre voie de routage par défaut pour le trafic de gestion. Notez que le trafic provenant du périphérique utilise par défaut la table de routage de gestion uniquement ou de données, en fonction du type, mais qu'il revient à l'autre table de routage si aucune route n'est trouvée. Les routes par défaut correspondront toujours au trafic et empêcheront un recours à l'autre table de routage. Dans ce cas, vous devez préciser l'interface que vous souhaitez utiliser pour le trafic de sortie si cette interface ne figure pas dans la table de routage par défaut.

Routes statiques

Vous pourriez souhaiter utiliser des routes statiques dans les cas suivants :

- Vos réseaux utilisent un protocole de découverte de routeur non pris en charge.
- Votre réseau est de petite taille et vous pouvez facilement gérer des routes statiques.
- Vous ne voulez pas associer le trafic ou la surcharge de la CPU aux protocoles de routage.
- Dans certains cas, une route par défaut ne suffit pas. La passerelle par défaut peut ne pas être en mesure d'atteindre le réseau de destination, vous devez donc également configurer des routes statiques plus spécifiques. Par exemple, si la passerelle par défaut est externe, la voie de routage par défaut ne peut pas diriger le trafic vers des réseaux internes qui ne sont pas directement connectés à ASA.
- Vous utilisez une fonctionnalité qui ne prend pas en charge les protocoles de routage dynamique.

Routage vers l'interface null0 pour abandonner le trafic indésirable

Les règles d'accès vous permettent de filtrer les paquets en fonction des informations contenues dans leurs en-têtes. Une voie de routage statique vers l'interface null0 est une solution complémentaire aux règles d'accès. Vous pouvez utiliser une route null0 pour transférer le trafic indésirable ou indésirable afin que le trafic soit abandonné.

Les routes statiques Null0 ont un profil de rendement positif. Vous pouvez également utiliser des routes statiques null0 pour éviter les boucles de routage. BGP peut tirer parti de la route statique null0 pour le routage trou noir déclenché à distance.

Priorités de routage

- Les routes qui identifient une destination spécifique prévalent sur la route par défaut.
- Lorsque plusieurs routages existent vers la même destination (statique ou dynamique), la distance administrative du routage détermine la priorité. Les routes statiques sont définies à 1, ce sont donc généralement les routes les plus prioritaires.
- Lorsque vous avez plusieurs routes statiques vers la même destination avec la même distance administrative, consultez Routage à chemins multiples à coûts égaux (ECMP), à la page 948.
- Pour le trafic sortant d'un tunnel avec l'option tunnelisé, cette voie de routage remplace toute autre voie de routage par défaut configurée ou apprise.

Routages en mode de pare-feu transparent et de groupes de ponts

Pour le trafic qui provient du ASA et est destiné à travers une interface membre de groupe de ponts pour un réseau non connecté directement, vous devez configurer une voie de routage par défaut ou des routes statiques pour que l'ASA sache de quelle interface membre de groupe de ponts envoyer trafic. Le trafic provenant de ASA peut inclure des communications avec un serveur syslog ou SNMP. Si certains serveurs ne peuvent pas être atteints par une seule route par défaut, vous devez configurer des routes statiques. Pour le mode transparent, vous ne pouvez pas spécifier les BVI comme interface de passerelle; seules les interfaces membres peuvent être utilisées. Pour les groupes de ponts en mode routé, vous devez préciser le BVI dans une voie de routage

statique; vous ne pouvez pas définir d'interface membre. Consultez Recherches d'adresse MAC ou de route, à la page 204 pour de plus amples renseignements.

Suivi du routage statique

L'un des problèmes des routes statiques est qu'il n'y a pas de mécanisme inhérent pour déterminer si la route est active ou inactive. Les routes statiques restent dans la table de routage même si la passerelle du saut suivant n'est plus disponible. Les routes statiques ne sont supprimées de la table de routage que si l'interface associée ASA tombe en panne.

La fonction de suivi de route statique fournit une méthode de suivi de la disponibilité d'une route statique et d'installation d'une route de secours en cas de défaillance de la route principale. Par exemple, vous pouvez définir une route par défaut vers une passerelle de FAI et une route de secours par défaut vers un FAI secondaire au cas où le FAI principal deviendrait indisponible.

L'ASA met en œuvre le suivi de route statique en associant une route statique à un hôte cible de surveillance sur le réseau de destination que l'ASA surveille à l'aide des demandes Echo ICMP. Si aucune réponse écho n'est reçue dans un délai donné, l'hôte est considéré comme hors service et la route associée est supprimée de la table de routage. Une route de secours non suivie avec une métrique plus élevée est utilisée à la place de la route supprimée.

Lorsque vous sélectionnez une cible de surveillance, vous devez vous assurer qu'elle peut répondre aux demandes d'écho ICMP. La cible peut être n'importe quel objet réseau de votre choix, mais vous pouvez envisager d'utiliser les objets suivants :

- L'adresse de la passerelle du FAI, pour la prise en charge du double FAI.
- L'adresse de passerelle du saut suivant, si vous êtes préoccupé par la disponibilité de la passerelle.
- Un serveur sur le réseau cible, tel qu'un serveur syslog, avec lequel l'ASA doit communiquer.
- Un objet réseau persistant sur le réseau de destination

Remarque Un poste de travail qui peut être éteint la nuit n'est pas un bon choix.

Vous pouvez configurer le suivi de routage statique pour les routes définies de manière statique ou pour les routages par défaut obtenus par DHCP ou PPPoE. Vous pouvez uniquement activer les clients PPPoE sur plusieurs interfaces avec le suivi de routage configuré.

Lignes directrices pour les routages statiques et par défaut

Mode de pare-feu et groupes de ponts

- En mode transparent, les routes statiques doivent utiliser l'interface du membre du groupe de ponts comme passerelle; vous ne pouvez pas préciser les BVI.
- En mode routé, vous devez spécifier les BVI comme passerelle; vous ne pouvez pas définir l'interface membre.

- Le suivi de routage statique n'est pas pris en charge pour les interfaces membres des groupes de ponts ou sur les BVI.

Adresse réseau prise en charge

- Le suivi de routage statique n'est pas pris en charge pour IPv6.
- L'ASA ne prend pas en charge le routage de classe E, donc un réseau de classe E n'est pas routable dans les routes statiques.

Mise en grappe et mode de contexte multiple

- Dans la mise en grappe, le suivi de routage statique n'est pris en charge que sur le nœud de contrôle.
- Le suivi de routage statique n'est pas pris en charge en mode de contexte multiple.

Entrées de routage ASP et RIB

Tous les routages et leur distance installés sur le périphérique sont capturés dans la table de routage ASP. Cette situation est commune à tous les protocoles de routage statiques et dynamiques. Seule la meilleure distance de routage est saisie dans le tableau RIB.

Configurer les routes par défaut et statiques

Vous devez configurer au moins une route par défaut. Vous devrez peut-être également configurer des routes statiques. Dans cette section, nous allons configurer une route par défaut, configurer une route statique et suivre une route statique.

Configurer une route par défaut

Une voie de routage par défaut est simplement une voie de routage statique avec 0.0.0.0/0 comme adresse IP de destination. Vous devez toujours avoir une route par défaut, soit configurée manuellement avec cette procédure, soit dérivée d'un serveur DHCP ou d'un autre protocole de routage.

Avant de commencer

Consultez les consignes suivantes pour l'option Tunneled (Tunnélisé) :

- N'activez pas la fonction de monodiffusion RPF (commande**ip verify reverse-path**) sur l'interface de sortie d'une route tunnellisée, car ce paramètre entraîne l'échec de la session.
- N'activez pas l'interception TCP sur l'interface de sortie de la route tunnellisée, car ce paramètre fait échouer la session.
- N'utilisez pas les moteurs d'inspection VoIP (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), la plateforme d'inspection DNS ou la plateforme d'inspection d'appel RPC DCE avec des routes tunnellisées, car ces moteurs d'inspection ignorent la route tunnellisée.
- Vous ne pouvez pas définir plusieurs routes par défaut avec l'option tunnellisée.
- ECMP pour le trafic en tunnel n'est pas pris en charge.

- Les routes tunnellisées ne sont pas prises en charge pour les groupes de ponts, qui ne prennent pas en charge la terminaison VPN pour le trafic traversant.

Procédure

Ajoutez une route par défaut :

IPv4 :

route *if_name* **0.0.0.0 0.0.0.0** *gateway_ip* [**distance**] [**tunneled**]

IPv6 :

ipv6 route *if_name* **::/0** *gateway_ip* [**distance**] [**tunneled**]

Exemple :

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1
```

L'*if_name* est l'interface par laquelle vous souhaitez envoyer le trafic spécifique. Pour le mode transparent, spécifiez un nom d'interface de membre de groupe de ponts. Pour le mode routé avec groupes de ponts, spécifiez le nom des BVI.

L'argument *distance* correspond à la distance administrative de la route, entre 1 et 254. La valeur par défaut est **1** si vous ne spécifiez pas de valeur. La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. La distance administrative par défaut pour les routes statiques est de 1, ce qui lui donne priorité sur les routes découvertes par les protocoles de routage dynamique, mais pas sur les routes directement connectées. La distance administrative par défaut pour les routes découvertes par OSPF est de 110. Si une route statique a la même distance administrative qu'une route dynamique, les routes statiques prévalent. Les routes connectées ont toujours la priorité sur les routes statiques ou découvertes dynamiquement.

Remarque
Pour le trafic direct, si vous avez deux routes par défaut configurées sur des interfaces différentes qui ont des mesures différentes, la connexion à l'ASA établie à partir de l'interface à mesure supérieure échoue, mais les connexions à l'ASA à partir de l'interface à mesure inférieure réussissent comme prévu. Pour le trafic en provenance de la boîte, si vous avez deux routes par défaut configurées sur différentes interfaces qui ont des mesures différentes, les deux interfaces peuvent être utilisées pour le trafic en provenance de la boîte, selon l'interface qui a été utilisée pour la connexion entrante.

Vous pouvez définir une route par défaut distincte pour le trafic VPN si vous souhaitez que votre trafic VPN utilise une route par défaut différente de celle du trafic non VPN à l'aide du mot clé **tunneled**. Par exemple, le trafic entrant des connexions VPN peut être facilement dirigé vers les réseaux internes, tandis que le trafic des réseaux internes peut être dirigé vers l'extérieur. Lorsque vous créez une route par défaut avec l'option tunnelisé, tout le trafic provenant d'un tunnel se terminant sur l'ASA qui ne peut pas être acheminé à l'aide de routes apprises ou statiques est envoyé vers cette route. Cette option n'est pas prise en charge pour les groupes de ponts.

Astuces

Vous pouvez saisir **0 0** au lieu de **0.0.0.0 0.0.0.0** pour l'adresse réseau de destination et le masque, comme le montre l'exemple suivant : **route outside 0 0 192.168.2.4**

Configurer une route statique

Une voie de routage statique définit où envoyer le trafic pour des réseaux de destination spécifiques.

Procédure

Ajoutez une route statique :

IPv4 :

route *if_name dest_ip mask gateway_ip* [**distance**]

IPv6 :

ipv6 route *if_name dest_ipv6_prefix/prefix_length gateway_ip* [**distance**]

Exemple :

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# ipv6 route outside 2001:DB8:1::0/32 2001:DB8:0:CC00::1
```

L'*if_name* est l'interface par laquelle vous souhaitez envoyer le trafic spécifique. Pour abandonner le trafic indésirable, saisissez l'interface **null0**. Pour le mode transparent, spécifiez un nom d'interface de membre de groupe de ponts. Pour le mode routé avec groupes de ponts, spécifiez le nom des BVI.

Les arguments *dest_ip* et *mask* ou *dest_ipv6_prefix/prefix_length* indiquent l'adresse IP du réseau de destination et l'argument *gateway_ip* est l'adresse du routeur de saut suivant. Les adresses que vous spécifiez pour la route statique sont les adresses qui sont dans le paquet avant d'entrer dans l'ASA et d'effectuer la NAT.

L'argument *distance* correspond à la distance administrative de la route. La valeur par défaut est **1** si vous ne spécifiez pas de valeur. La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. La distance administrative par défaut pour les routes statiques est de 1, ce qui lui donne priorité sur les routes découvertes par les protocoles de routage dynamique, mais pas sur les routes directement connectées. La distance administrative par défaut pour les routes découvertes par OSPF est de 110. Si une voie de routage statique a la même distance administrative qu'une voie de routage dynamique, la voie statique prévaut. Les routes connectées ont toujours la priorité sur les routes statiques ou découvertes dynamiquement.

Exemple

L'exemple suivant montre les routes statiques pour trois réseaux qui vont à la même passerelle et un autre réseau qui va à une passerelle distincte :

```
route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
```

```
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1
```

Configurer le suivi de route statique

Pour configurer le suivi des routes statiques, procédez comme suit.

Procédure

Étape 1 Configurez la route statique pour l'interface (externe 1) utilisée pour atteindre le réseau :

```
ciscoasa(config)# route outside1 172.29.139.134 255.255.255.255 10.0.0.1
```

Étape 2 Définissez le processus de surveillance :

sla monitor sla_id

Exemple :

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

Étape 3 Spécifiez le protocole de surveillance, l'hôte cible sur le réseau suivi et l'interface par laquelle vous accédez au réseau :

type echo protocol ipicmpecho target_ip **interface** if_name

Exemple :

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134 interface outside1
ciscoasa(config-sla-monitor-echo)#
```

L'argument *target_ip* est l'adresse IP de l'objet réseau dont le processus de suivi surveille la disponibilité. Pendant que cet objet est disponible, la route du processus de suivi est installée dans la table de routage. Lorsque cet objet n'est plus disponible, le processus de suivi supprime la route et la route de secours est utilisée à sa place.

Étape 4 (Facultatif) Configurez les options de surveillance. Consultez la référence de commande pour les commandes suivantes : **frequency, num-packets, request-data-size, threshold, timeout** et **tos**.

Étape 5 Planifiez le processus de surveillance :

sla monitor schedule sla_id [**life** {**forever** | seconds}] [**start-time** {hh:mm [:ss] [month day | day month] | **pending** | **now** | **after** hh:mm:ss}] [**ageout** seconds] [**recurring**]

Exemple :

```
ciscoasa(config)# sla monitor schedule 5 life forever start-time now
```

En règle générale, vous utiliserez la commande **sla monitor schedule** *sla_id* **life forever start-time now** pour le calendrier de surveillance et permettrez à la configuration de surveillance de déterminer la fréquence des tests.

Cependant, vous pouvez planifier ce processus de surveillance pour qu'il commence dans le futur et qu'il se produise uniquement à des heures spécifiées.

Étape 6 Associez une route statique suivie au processus de surveillance du SLA :

track track_id **rtr** sla_id **reachability**

Exemple :

```
ciscoasa(config)# track 6 rtr 5 reachability
```

L'argument *track_id* est un numéro de suivi que vous attribuez avec cette commande. L'argument *sla_id* est le numéro d'identifiant du processus SLA.

Étape 7 Suivez l'un des types de route suivants :

- Route statique :

  route if_name dest_ip mask gateway_ip [distance] **track** track_id

  Exemple :

  ```
  ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
  ```

  Vous ne pouvez pas utiliser l'option **tunneled**.

- Route par défaut obtenue par DHCP :

  ```
  interface interface_id
    dhcp client route track track_id
    ip address dhcp setroute
  ```

- Route par défaut obtenue par PPPoE :

  ```
  interface interface_id
    pppoe client route track track_id
    ip address pppoe setroute
  ```

Étape 8 Créez une route de secours non suivie.

La route de secours est une route statique vers la même destination que la route suivie, mais via une interface ou une passerelle différente. Vous devez attribuer à cette route une distance administrative (mesure) plus élevée que votre route suivie.

Supervision d'une route statique ou par défaut

- **afficher route**

Affiche la table de routage.

Exemples de routes statiques ou par défaut

L'exemple suivant montre comment créer une route statique qui envoie tout le trafic destiné à 10.1.1.0/24 au routeur 10.1.2.45, qui est connecté à l'interface interne, définit trois routes statiques à coût égal qui dirigent le trafic vers trois passerelles différentes sur l'interface DMZ, et ajoute une route par défaut pour le trafic tunnelé et une autre pour le trafic normal.

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

Historique des routes statiques et par défaut

Tableau 36 : Historique des fonctionnalités pour les routes statiques et par défaut

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Suivi du routage statique	7.2(1)	La fonction de suivi de route statique fournit une méthode de suivi de la disponibilité d'une route statique et d'installation d'une route de secours en cas de défaillance de la route principale. Nous avons ajouté les commandes suivantes : **clear configure sla, frequency, num-packets, request-data-size, show sla monitor, show running-config sla, sla monitor, sla monitor schedule, threshold, timeout, tos, track rtr**
Route statique null0 pour abandonner le trafic	9.2(1)	L'envoi du trafic vers une interface null0 entraîne l'abandon des paquets destinés au réseau spécifié. Cette fonctionnalité est utile dans la configuration de Remotely Triggered Black Hole (RTBH) pour BGP. Nous avons modifié la commande suivante : **route**.



CHAPITRE 29

Routage basé sur une stratégie

Ce chapitre décrit comment configurer l'ASA pour prendre en charge le routage basé sur les politiques (BPR). Les sections suivantes décrivent le routage basé sur les politiques, les lignes directrices relatives au PBR et la configuration du PBR.

- À propos du routage basé sur les politiques, à la page 961
- Lignes directrices pour le routage basé sur des politiques, à la page 963
- Configurer le routage basé sur les politiques, à la page 965
- Exemples de routage basé sur des politiques, à la page 969
- Historique du routage basé sur des politiques, à la page 978

À propos du routage basé sur les politiques

Le routage traditionnel est basé sur la destination, ce qui signifie que les paquets sont acheminés en fonction de l'adresse IP de destination. Cependant, il est difficile de modifier le routage d'un trafic spécifique dans un système de routage basé sur la destination. Avec le routage basé sur les politiques (PBR), vous pouvez définir le routage en fonction de critères autres que le réseau de destination. Le PBR vous permet d'acheminer le trafic en fonction de l'adresse source, du port source, de l'adresse de destination, du port de destination, du protocole ou d'une combinaison de ces éléments.

Routage basé sur les politiques :

- Vous permet de fournir une qualité de service (QoS) à un trafic différencié.
- Vous permet de répartir le trafic interactif et par lots sur des chemins permanents à faible bande passante et à faible coût et des chemins commutés à bande passante élevée et à coût élevé.
- Permet aux fournisseurs de services Internet et à d'autres organisations d'acheminer le trafic provenant de divers ensembles d'utilisateurs par le biais de connexions Internet bien définies.

Le routage basé sur les politiques peut mettre en œuvre la QoS en classant et en marquant le trafic à la périphérie du réseau, puis en utilisant le PBR dans tout le réseau pour acheminer le trafic marqué le long d'un chemin spécifique. Cela permet le routage de paquets provenant de différentes sources vers différents réseaux, même lorsque les destinations sont les mêmes, et cela peut être utile pour interconnecter plusieurs réseaux privés.

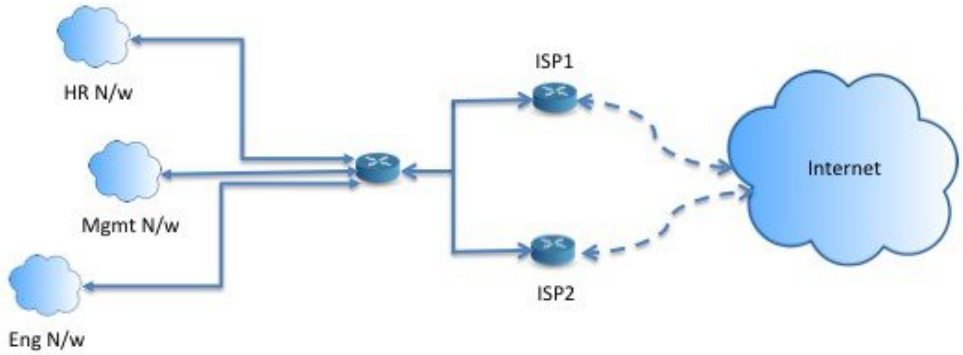
Pourquoi utiliser le routage basé sur des politiques?

Imaginez une entreprise qui dispose de deux liaisons entre des sites : l'une, une liaison onéreuse à bande passante élevée et à faible délai, et l'autre, à faible bande passante, avec un délai plus élevé et un moindre coût. Lors de l'utilisation de protocoles de routage traditionnels, la liaison à plus grande largeur de bande recevrait la majeure partie, voire la totalité, du trafic qui y est envoyé, en fonction des économies de métriques obtenues grâce aux caractéristiques de la bande passante et/ou du délai (avec EIGRP ou OSPF) de la liaison. PBR vous permet d'acheminer le trafic de priorité supérieure sur la liaison à bande passante élevée/faible délai, tout en envoyant tout le reste du trafic sur la liaison à bande passante faible/délai élevé.

Certaines applications du routage basé sur les politiques sont les suivantes :

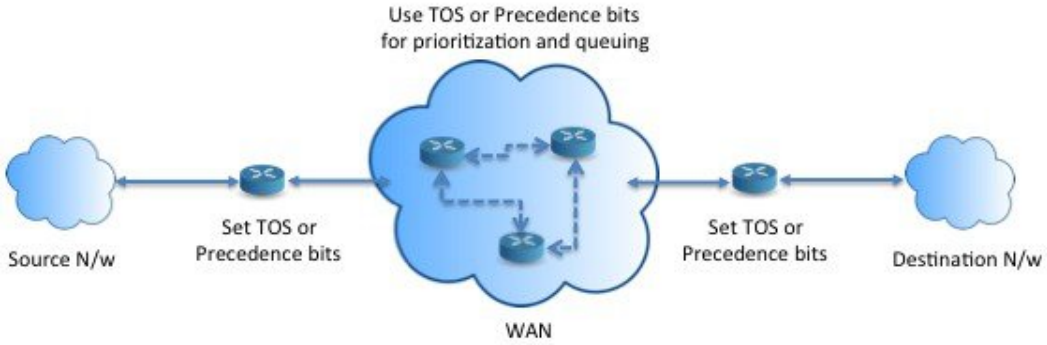
Routage à accès égal et sensible à la source

Dans cette topologie, le trafic provenant du réseau RH et du réseau de gestion peut être configuré pour passer par FAI1, et le trafic du réseau des ingénieurs peut être configuré pour passer par FAI2. Ainsi, le routage basé sur les politiques permet aux administrateurs réseau de fournir un routage à accès égal et sensible à la source, comme indiqué ici.



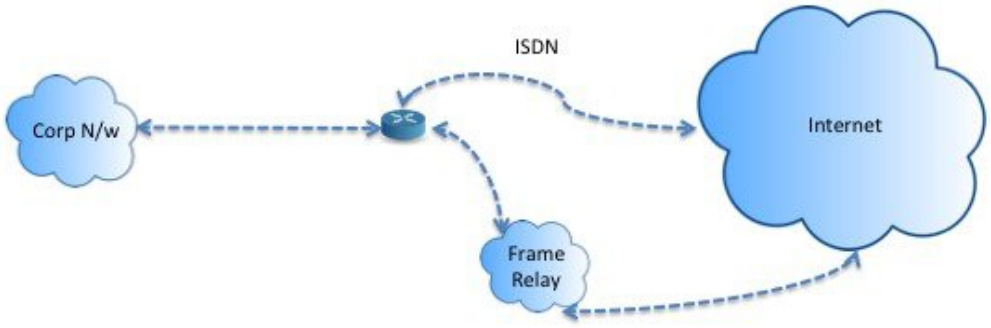
Qualité de service

En balisant les paquets avec le routage basé sur les politiques, les administrateurs réseau peuvent classer le trafic réseau au périmètre du réseau pour différentes classes de service, puis mettre en œuvre ces classes de service au cœur du réseau à l'aide de la mise en file d'attente de priorité, personnalisée ou pondérée (comme indiqué dans la figure ci-dessous). Cette configuration améliore les performances du réseau en éliminant le besoin de classer le trafic explicitement sur chaque interface WAN au cœur du réseau fédérateur.



Réduction des coûts

Une organisation peut diriger le trafic en bloc associé à une activité spécifique pour utiliser un lien à haute bande passante à coût élevé pendant une durée courte et maintenir la connectivité de base sur un lien à faible coût à bande passante inférieure pour le trafic interactif en définissant la topologie, comme indiqué ici.



Partage de la charge

En plus des fonctionnalités de partage dynamique de charge offertes par l'équilibrage de charge ECMP, les administrateurs réseau peuvent désormais mettre en œuvre des politiques pour répartir le trafic entre plusieurs chemins en fonction des caractéristiques du trafic.

Par exemple, dans la topologie décrite dans le scénario de routage à accès égalitaire sensible, un administrateur peut configurer le routage basé sur une politique pour partager la charge du trafic provenant du réseau des Ressources humaines par ISP1 et du trafic provenant du réseau Eng par ISP2.

Mise en œuvre de PBR

L'ASA utilise les ACL pour faire correspondre le trafic et effectuer des actions de routage sur le trafic. Plus précisément, vous configurez une carte de routage qui spécifie une ACL pour la correspondance, puis vous spécifiez une ou plusieurs actions pour ce trafic. Enfin, vous associez la carte de routage à une interface sur laquelle vous souhaitez appliquer le PBR à tout le trafic entrant.

Remarque Avant de procéder à la configuration, assurez-vous que le trafic d'entrée et de sortie de chaque session traverse la même interface destinée au fournisseur de services Internet pour éviter les comportements imprévus causés par le routage asymétrique, en particulier lorsque la NAT et le VPN sont utilisés.

Lignes directrices pour le routage basé sur des politiques

Mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Routage par flux

Étant donné que l'ASA effectue le routage par flux, le routage des politiques est appliqué sur le premier paquet et la décision de routage qui en résulte est stockée dans le flux créé pour le paquet. Tous les paquets suivants appartenant à la même connexion correspondent simplement à ce flux et sont acheminés de manière appropriée.

Politiques PBR non appliquées pour la recherche de route de sortie

Le routage basé sur des règles est une fonction d'entrée uniquement, c'est-à-dire qu'il n'est appliqué qu'au premier paquet d'une nouvelle connexion entrante, et c'est à ce moment-là que l'interface de sortie est sélectionnée pour le tronçon d'aller de la connexion. Notez que PBR ne sera pas déclenché si le paquet entrant appartient à une connexion existante ou si la NAT est appliquée et que cette dernière choisit l'interface de sortie.

Politiques PBR non appliquées pour le trafic amorce



Remarque Il y a connexion amorce lorsque l'établissement de liaison nécessaire entre la source et la destination n'a pas lieu.

Lorsqu'une nouvelle interface interne est ajoutée et qu'une nouvelle politique VPN est créée à l'aide d'un groupement d'adresses unique, le PBR est appliqué à l'interface externe correspondant à la source du nouveau groupement de clients. Ainsi, PBR envoie le trafic du client au prochain saut sur la nouvelle interface. Cependant, PBR n'est pas impliqué dans le trafic de retour d'un hôte qui n'a pas encore établi de connexion avec les nouvelles routes d'interface interne vers le client. Ainsi, le trafic de retour de l'hôte vers le client VPN, en particulier la réponse du client VPN, est abandonné car il n'y a aucune voie de routage valide. Vous devez configurer une voie de routage statique pondérée avec une métrique plus élevée sur l'interface interne.

Mise en grappe

- La mise en grappe est prise en charge.
- Dans un scénario de grappe, sans routes statiques ou dynamiques, et avec la commande ip-verify-reverse path activée, le trafic asymétrique peut être abandonné. Il est donc conseillé de désactiver ip-verify-reverse path.

Prise en charge d'IPv6

IPv6 est pris en charge.

Lignes directrices relatives à la surveillance des chemins d'accès

Voici les lignes directrices pour configurer la surveillance des chemins d'accès sur les interfaces :

- Les interfaces doivent avoir un nom d'interface.
- Les interfaces de gestion uniquement ne peuvent pas être configurées avec la surveillance des chemins d'accès. Pour configurer la surveillance des chemins d'accès, vous devez décocher la case **Dedicate this interface to management only** (Dédier cette interface à la gestion uniquement).
- La surveillance des chemins d'accès n'est pas prise en charge sur les périphériques en mode de système transparent ou de contexte multiple.

- Les types de surveillance automatique (auto, auto4 et auto6) ne sont pas pris en charge pour les interfaces de tunnel.
- La surveillance des chemins d'accès ne peut pas être configurée pour les interfaces suivantes :
  - BVI
  - Boucle avec retour
  - DVTI

Directives supplémentaires

- Toutes les restrictions et limites de configuration existantes liées aux cartes de routage seront conservées.
- N'utilisez pas de cartes de routage contenant des listes de correspondance de politiques pour le routage basé sur des politiques. La liste de politiques de correspondance est uniquement utilisée pour le BGP.
- Le transfert de chemin inverse de monodiffusion (uRPF) valide l'adresse IP source des paquets reçus sur une interface par rapport à la table de routage et non par rapport à la carte de routage PBR. Lorsque uRPF est activé, les paquets reçus sur une interface par l'intermédiaire de PBR sont abandonnés tels qu'ils sont, sans l'entrée de route spécifique. Par conséquent, lorsque vous utilisez PBR, assurez-vous de désactiver uRPF.

Configurer le routage basé sur les politiques

Une carte de routage est composée d'une ou de plusieurs instructions route-map. Chaque instruction a un numéro de séquence, ainsi qu'une clause allow ou deny. Chaque instruction route-map contient des commandes match et set. La commande match indique les critères de correspondance à appliquer au paquet. La commande set indique l'action à entreprendre sur le paquet.

- Lorsqu'une carte de routage est configurée avec des clauses match/set IPv4 et IPv6 ou lorsqu'une ACL unifiée faisant correspondre le trafic IPv4 et IPv6 est utilisée, les actions définies seront appliquées en fonction de la version IP de destination.
- Lorsque plusieurs interfaces ou sauts suivants sont configurés en tant qu'action définie, toutes les options sont évaluées l'une après l'autre jusqu'à ce qu'une option utilisable valide soit trouvée. Aucun équilibrage de charge ne sera effectué parmi les multiples options configurées.
- L'option verify-availability n'est pas prise en charge en mode de contexte multiple.

Procédure

Étape 1 Définissez une liste d'accès standard ou étendue :

access-list *name* **standard** {**permit** | **deny**} {**any4** | **host** *ip_address* | *ip_address mask*}

access-list *name* **extended** {**permit** | **deny**} *protocol source_and_destination_arguments*

Exemple :

```
ciscoasa(config)# access-list testacl extended permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
```

Si vous utilisez une liste de contrôle d'accès standard, la mise en correspondance s'effectue uniquement pour l'adresse de destination. Si vous utilisez une liste de contrôle d'accès étendue, vous pouvez mettre en correspondance la source, la destination ou les deux.

Pour la liste de contrôle d'accès étendue, vous pouvez spécifier les paramètres IPv4, IPv6, Identity Firewall ou Cisco TrustSec. Vous pouvez également inclure des objets de service réseau. Pour obtenir la syntaxe complète, consultez la référence de commande ASA.

Étape 2 Créez une entrée de carte de routage :

route-map *nom* {**permis** | **refuser**} [*numéro_séquence*]

Exemple :

```
ciscoasa(config)# route-map testmap permit 12
```

Les entrées de carte de routage sont lues dans l'ordre. Vous pouvez identifier l'ordre à l'aide de l'argument *sequence_number* ou l'ASA utilise l'ordre dans lequel vous ajoutez les entrées de la carte de routage.

La liste de contrôle d'accès comprend également ses propres instructions d'autorisation et de refus. Pour les correspondances Autoriser/Autoriser entre la carte de routage et la liste de contrôle d'accès, le traitement de routage basé sur les politiques se poursuit. Pour les correspondances Autoriser/refuser, le traitement se termine pour cette carte de routage et les autres cartes de routage sont vérifiées. Si le résultat est toujours Autoriser/refuser, la table de routage normale est utilisée. Pour les correspondances refus/refus, le traitement de routage basé sur les politiques se poursuit.

Remarque
Lorsqu'une carte de routage est configurée sans action Allow ou Deny (autoriser ou refuser) et sans numéro de séquence, elle suppose par défaut que l'action est l'autorisation et le numéro de séquence est 10.

Étape 3 Définissez les critères de correspondance à appliquer à l'aide d'une liste d'accès :

match ip address *access-list_name* [*access-list_name*...]

Exemple :

```
ciscoasa(config-route-map)# match ip address testacl
```

Remarque
Vérifiez que la liste d'accès ne contient aucune règle inactive. Vous ne pouvez pas définir une correspondance ACL avec les règles inactives sur un PBR.

Étape 4 Configurez une ou plusieurs actions définies :

- Définissez l'adresse de saut suivant :

  set {ip | ipv6} next-hop *ipv4_or_ipv6_address*

  Vous pouvez configurer plusieurs adresses IP de saut suivant, auquel cas elles sont évaluées dans l'ordre spécifié jusqu'à ce qu'une adresse IP de saut suivant routable soit trouvée. Les prochains sauts configurés doivent être connectés directement; Sinon, l'action définie ne sera pas appliquée.

- Définissez l'adresse de saut suivant :

  set {ip | ipv6} default next-hop *ipv4_or_ipv6_address*

  Si la recherche normale de route échoue pour le trafic correspondant, l'ASA transfère le trafic en utilisant l'adresse IP de saut suivant spécifiée.

- Définir une adresse IPv4 du saut suivant récursive :

  set ip next-hop recursive *ip_address*

  Les deux commandes **set ip next-hop** et **set ip default next-hop** exigent que le prochain saut se trouve sur un sous-réseau directement connecté. Avec **set ip next-hop recursive**, l'adresse de saut suivant n'a pas besoin d'être connectée directement. Au lieu de cela, une recherche récursive est effectuée sur l'adresse de saut suivant, et le trafic correspondant est transmis au saut suivant utilisé par cette entrée de routage en fonction du chemin de routage utilisé sur le routeur.

- Vérifiez si les prochains sauts IPv4 d'une carte de routage sont disponibles :

  set ip next-hop verify-availability *next-hop-address sequence_number* **track** *object*

  Vous pouvez configurer un objet de suivi de moniteur SLA pour vérifier l'accessibilité du prochain saut. Pour vérifier la disponibilité de plusieurs prochains sauts, plusieurs commandes **set ip next-hop verify-availability** peuvent être configurées avec différents numéros de séquence et différents objets de suivi.

- Définissez l'interface de sortie du paquet :

  set interface *interface_name*

  ou

  set interface null0

  Cette commande configure l'interface par laquelle le trafic correspondant est transféré. Vous pouvez configurer plusieurs interfaces, auquel cas elles sont évaluées dans l'ordre spécifié jusqu'à ce qu'une interface valide soit trouvée. Lorsque vous spécifiez **null0**, tout le trafic correspondant à la carte de routage sera abandonné. Il doit y avoir une voie de routage pour la destination qui peut être acheminée par l'interface spécifiée (statique ou dynamique).

- Définissez l'interface de sortie en fonction de son coût :

  set adaptive-interface cost *interface_list*

  L'interface de sortie est sélectionnée dans la liste des interfaces séparées par des espaces. Si les coûts des interfaces sont les mêmes, il s'agit d'une configuration active-active et les paquets sont équilibrés (round robin) sur les interfaces de sortie. Si les coûts sont différents, l'interface avec le coût le plus faible est sélectionnée. Les interfaces ne sont prises en compte que si elles sont actives. Par exemple :

  ```
  set adaptive-interface cost output1 output2
  ```

- Définissez l'interface par défaut sur null0 :

  set default interface null0

  Si une recherche de route normale échoue, l'ASA transfère le trafic null0 et le trafic sera abandonné.

- Définissez la valeur de bit Ne pas fragmenter (DF) dans l'en-tête IP :

  set ip df {0|1}

- Classez le trafic IP en définissant un point de code de services différentiels (DSCP) ou une valeur de priorité IP dans le paquet :

  set {ip | ipv6} dscp *new_dscp*

Remarque
Lorsque plusieurs actions de définition sont configurées, l'ASA les évalue dans l'ordre suivant : **set ip next-hop verify-availability; set ip next-hop**; **set ip next-hop recursive**; **set interface; set adaptive-interface cost**; **set ip default next-hop**; **set default interface**.

Étape 5 Configurez une interface et passez en mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
```

Étape 6 Si vous utilisez **set adaptive-interface cost** comme critères dans la carte de routage, définissez le coût sur l'interface :

policy-route cost *value*

La valeur peut être 1 à 65535. La valeur par défaut est 0, et vous pouvez la réinitialiser en utilisant la version **no** de la commande. Plus le numéro de priorité est faible, plus la priorité est élevée. Par exemple, 1 a priorité sur 2.

Lorsque vous définissez le coût de routage de politique et que vous utilisez la commande **set adaptive-interface cost** dans la carte de routage, le trafic de sortie fait l'objet d'un équilibre de charge à tour de rôle sur les interfaces sélectionnées (en supposant qu'elles soient actives) qui ont le même coût d'interface. Si les coûts sont différents, les interfaces les plus coûteuses sont utilisées comme sauvegardes de l'interface la moins coûteuse.

Par exemple, en définissant le même coût pour deux liaisons WAN, vous pouvez équilibrer la charge du trafic sur ces liaisons afin d'améliorer peut-être les performances. Toutefois, si l'un des liens WAN a une bande passante plus élevée que l'autre, vous pouvez définir le coût de la liaison à bande passante supérieure à 1 et pour celui de la bande passante inférieure à 2, de sorte que le lien à bande passante inférieure ne soit utilisé que si le lien à bande passante la plus élevée est en panne.

Étape 7 Vous pouvez définir le type de surveillance pour l'homologue de l'interface afin de collecter les mesures flexibles :

policy-route path-monitoring {**IPv4** | **IPv6** | **auto** | **auto4** | **auto6**}

Où,

- **auto** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface, si elle existe (identique à Auto IPv4). Sinon, envoie à la passerelle par défaut IPv6 de l'interface (identique à Auto IPv6).
- **ipv4** : envoie les sondes ICMP à l'adresse IPv4 homologue spécifiée (IP du saut suivant) pour la surveillance.
- **ipv6** : envoie les sondes ICMP à l'adresse IPv4 homologue spécifiée (IP du saut suivant) pour la surveillance.
- **auto4** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface.

- **auto6** : envoie des sondes ICMP à la passerelle par défaut IPv6 de l'interface.

Exemple :

```
ciscoasa(config-if)# policy-route ?

interface mode commands/options:
  cost              set interface cost
  path-monitoring   Keyword for path monitoring
  route-map         Keyword for route-map
ciscoasa(config-if)# policy-route path-monitoring ?
interface mode commands/options:
  A.B.C.D     peer-ipv4
  X:X:X:X::X  peer-ipv6
  auto        Use remote peer IPv4/6 based on config
  auto4       Use only IPv4 address based on config
  auto6       Use only IPv6 address based on config

ciscoasa(config-if)# policy-route path-monitoring auto
```

Pour effacer les paramètres de surveillance de chemin d'accès sur l'interface, utilisez la commande **clear path-monitoring** :

Exemple :

```
clear path-montoring outside1
```

Étape 8 Configurez le routage basé sur les politiques pour le trafic traversant la boîte :

`policy-route route-map` *route_map_name*

Exemple :

```
ciscoasa(config-if)# policy-route route-map testmap
```

Pour supprimer une carte de routage basée sur les politiques existante, saisissez simplement la forme **no** de cette commande.

Exemple :

```
ciscoasa(config-if)# no policy-route route-map testmap
```

Exemples de routage basé sur des politiques

Les sections suivantes présentent des exemples de configuration de carte de routage, de routage basé sur des politiques, ainsi qu'un exemple spécifique de PBR en action.

Exemples de configuration de carte de routage

Dans l'exemple suivant, comme aucune action ni aucune séquence n'est spécifiée, une action implicite d'autorisation et un numéro de séquence de 10 sont supposés :

```
ciscoasa(config)# route-map testmap
```

Dans l'exemple suivant, comme aucun critère de correspondance n'est spécifié, une correspondance implicite « any » est présumée :

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10
```

Dans cet exemple, tout le trafic correspondant à <acl> sera acheminé selon la politique et transféré par l'intermédiaire d'une interface externe.

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
ciscoasa(config-route-map)# set interface outside
```

Dans cet exemple, aucune interface ni action de saut suivant n'étant configurée, tout le trafic correspondant à <acl> verra ses champs df bit et dscp modifiés conformément à la configuration et sera transféré selon le routage normal.

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
set ip df 1
set ip precedence af11
```

Dans l'exemple suivant, tout le trafic correspondant à <acl_1> est transféré à l'aide du saut suivant 1.1.1.10, tout le trafic correspondant <acl_2> est transféré à l'aide du saut suivant 2.1.1.10 et le reste du trafic est abandonné. L'absence de critères de « correspondance » implique une correspondance implicite « any ».

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl_1>
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address <acl_2>

ciscoasa(config-route-map)# set ip next-hop 2.1.1.10
ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# set interface Null0
```

Dans l'exemple suivant, l'évaluation de la carte de routage sera telle que (i) une action de carte de routage permit et une action acl permit appliqueront les actions définies (ii) une action de carte de routage deny et une action acl permit passeront à la recherche de route normale (iii) une action de carte de routage permit/deny et une action acl deny continueront avec l'entrée suivante de la carte de routage. Si aucune entrée de carte de routage suivante n'est disponible, nous reviendrons à la recherche de route normale.

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address permit_acl_1 deny_acl_2
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap deny 20
ciscoasa(config-route-map)# match ip address permit_acl_3 deny_acl_4
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10

ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# match ip address deny_acl_5
```

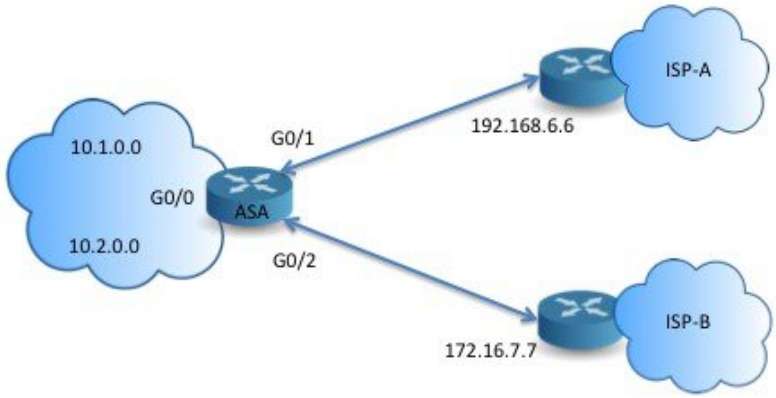
```
ciscoasa(config-route-map)# set interface outside
```

Dans l'exemple suivant, lorsque plusieurs actions définies sont configurées, elles sont évaluées dans l'ordre mentionné ci-dessus. Ce n'est que lorsque toutes les options d'une action définie sont évaluées et ne peuvent être appliquées que les actions définies suivantes seront prises en compte. Cet ordre garantira que le prochain saut le plus disponible et le moins distant sera essayé en premier, suivi du prochain saut le plus disponible et le moins distant, et ainsi de suite.

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address acl_1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.10 1 track 1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.11 2 track 2
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.12 3 track 3
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10 2.1.1.11 2.1.1.12
ciscoasa(config-route-map)# set ip next-hop recursive 3.1.1.10
ciscoasa(config-route-map)# set interface outside-1 outside-2
ciscoasa(config-route-map)# set ip default next-hop 4.1.1.10 4.1.1.11
ciscoasa(config-route-map)# set default interface Null0
```

Exemple de configuration pour PBR

Cette section décrit l'ensemble complet de configuration requis pour configurer PBR pour le scénario suivant :



Tout d'abord, nous devons configurer les interfaces.

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-1
ciscoasa(config-if)# ip address 192.168.6.5 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-2
ciscoasa(config-if)# ip address 172.16.7.6 255.255.255.0
```

Ensuite, nous devons configurer une liste d'accès pour la correspondance du trafic.

```
ciscoasa(config)# access-list acl-1 permit ip 10.1.0.0 255.255.0.0
ciscoasa(config)# access-list acl-2 permit ip 10.2.0.0 255.255.0.0
```

Nous devons configurer une carte de routage en spécifiant la liste d'accès ci-dessus comme critères de correspondance et les actions définies requises.

```
ciscoasa(config)# route-map equal-access permit 10
ciscoasa(config-route-map)# match ip address acl-1
ciscoasa(config-route-map)# set ip next-hop 192.168.6.6

ciscoasa(config)# route-map equal-access permit 20
ciscoasa(config-route-map)# match ip address acl-2
ciscoasa(config-route-map)# set ip next-hop 172.16.7.7

ciscoasa(config)# route-map equal-access permit 30
ciscoasa(config-route-map)# set ip interface Null0
```

Maintenant, cette carte de routage doit être associée à une interface.

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map equal-access
```

Pour afficher la configuration du routage des politiques.

```
ciscoasa(config)# show policy-route
Interface                  Route map
GigabitEthernet0/0   equal-access
```

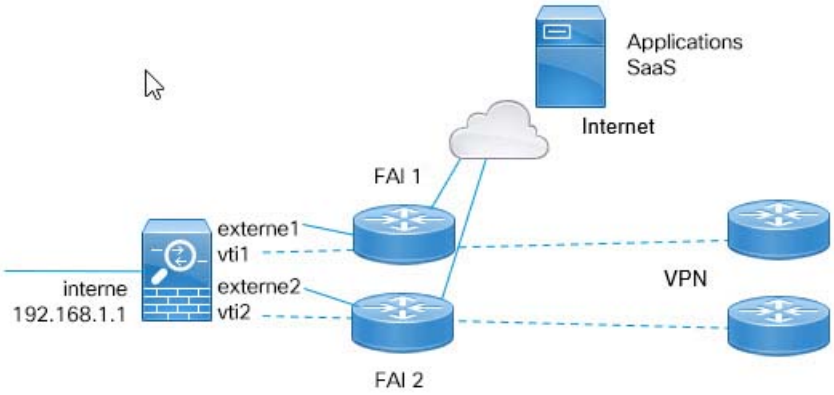
Accès Internet direct à l'aide du réseau WAN défini par logiciel

Un réseau de succursale typique utilise un VPN de site à site pour connecter la succursale à un concentrateur d'entreprise. Tout le trafic non local est ensuite acheminé vers le réseau de l'entreprise, où il est acheminé vers les services internes ou vers Internet, selon le cas.

Cette configuration crée un goulot d'étranglement au niveau du concentrateur de l'entreprise. Si du trafic de succursale est destiné à des services Internet, comme Google Search ou Gmail, il n'est pas nécessaire d'accéder d'abord au réseau d'entreprise avant d'accéder à Internet.

En utilisant le routage basé sur des politiques, vous pouvez plutôt configurer un accès Internet direct à partir de la succursale pour le trafic qui n'a pas besoin des services du réseau d'entreprise. Ainsi, le trafic vers Internet n'est pas envoyé au concentrateur de l'entreprise, et celui-ci n'a plus qu'à gérer le trafic destiné aux services internes du réseau d'entreprise. Cette configuration devrait améliorer les performances globales et le débit du réseau.

L'exemple suivant montre comment configurer l'accès Internet direct pour la configuration suivante, où deux interfaces externes se connectent à différents fournisseurs de services Internet et des interfaces de tunnel virtuel (VTI) hébergent des connexions VPN de site à site au réseau d'entreprise. L'exemple montre comment diriger le trafic destiné à certaines applications SaaS vers Internet et ainsi contourner le réseau d'entreprise.



Avant de commencer

Cet exemple suppose que vous avez déjà défini un VPN de site à site à l'aide d'interfaces de tunnel virtuel (VTI) définies sur les interfaces externes (orientées WAN) pour connecter la succursale au concentrateur de l'entreprise et que celui-ci fonctionne correctement. Le trafic acheminé vers les interfaces VTI est ainsi redirigé vers le réseau d'entreprise, tandis que le trafic acheminé directement vers les interfaces externes est acheminé vers Internet.

Cela suppose également que vous ayez configuré des serveurs DNS et activé la résolution DNS sur les interfaces de l'appareil. Utilisez la commande **show dns trusted-source detail** pour voir quels serveurs seront surveillés. Si vous souhaitez limiter les serveurs utilisés, utilisez la commande **no dns trusted-source** pour désactiver la surveillance de trafic sur les serveurs sélectionnés.

Procédure

Étape 1 Configurez les objets et les groupes de services réseau pour définir le trafic souhaité.

L'exemple suivant crée des objets pour définir Office365 et WebEx, puis crée un groupe d'objets SaaS_Applications pour les contenir. Vous devez créer un groupe d'objets, vous ne pouvez pas utiliser directement les objets dans une entrée de contrôle d'accès.

```
object network-service office365
    domain outlook.office365.com tcp eq 443
    domain onlineapps.live.com tcp eq 443
    domain skype.live.com tcp eq 443

object network-service webex
    domain webex.com tcp eq 443

object-group network-service SaaS_Applications
    network-service-member office365
    network-service-member webex
```

Étape 2 Créez une ACL étendue pour correspondre au trafic souhaité.

L'exemple suivant fait correspondre le trafic du réseau interne au groupe d'objets SaaS Applications.

```
access-list DIA_traffic extended permit ip 192.168.1.0 255.255.255.0
object-group-network-service SaaS_Applications
```

Étape 3 (Facultatif) Configurez le coût sur les interfaces de sortie.

En supposant que les interfaces output1 et output2 sont déjà configurées et fonctionnent, ajoutez simplement la commande policy-route cost. Cette étape est facultative si vous souhaitez configurer le système pour utiliser le traitement de circuit cyclique (round robin) pour équilibrer la charge sur les deux liaisons WAN de sortie. Cependant, vous devez définir les coûts si vous souhaitez créer une configuration active/de secours, dans laquelle une liaison est utilisée sauf si elle est hors service.

Voici un exemple de configuration active/active à coût égal.

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 1
```

Voici un exemple dans lequel output1 est la liaison préférée et output2 n'est utilisée que si output1 est hors service.

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 2
```

Étape 4 Créez une carte de routage pour faire correspondre l'ACL étendue et diriger le trafic en conséquence.

L'exemple suivant utilise la liste ACL pour faire correspondre le trafic, puis utilise le coût d'interface adaptatif pour diriger le trafic vers l'interface de sortie.

```
route-map mymap 10
  match ip address DIA_traffic
  set adaptive-interface cost outside1 outside2
```

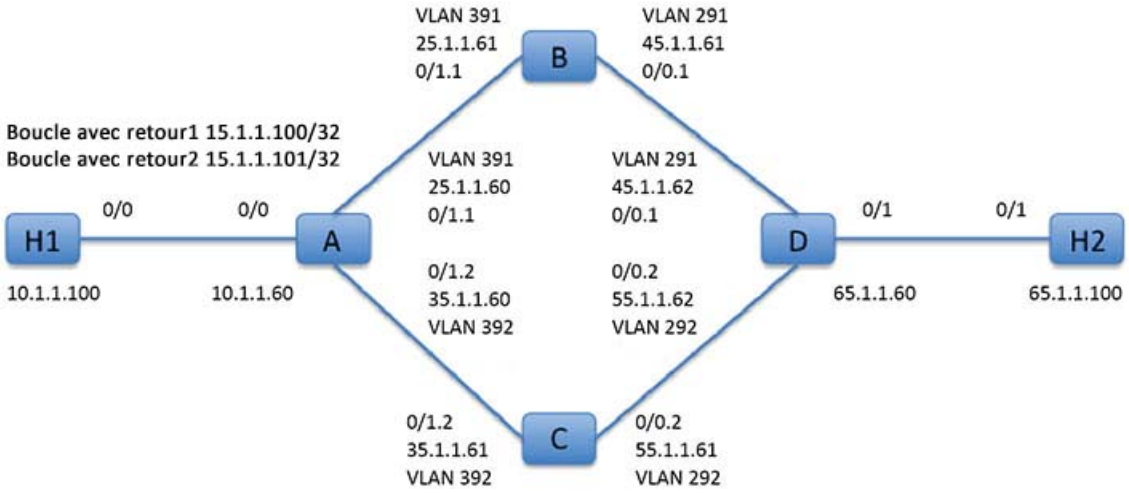
Étape 5 Configurez le routage basé sur des politiques sur l'interface d'entrée pour envoyer le trafic SaaS aux interfaces externes.

L'exemple suivant associe la carte de routage à l'interface interne pour activer le routage basé sur des politiques pour un accès Internet direct.

```
interface G1/0
  nameif inside
  policy-route route-map mymap
```

Routage basé sur des politiques en action

Nous utiliserons cette configuration de test pour configurer le routage basé sur des politiques avec différents critères de correspondance et définir des actions afin de voir comment elles sont évaluées et appliquées.



Tout d'abord, nous allons commencer par la configuration de base pour tous les périphériques impliqués dans l'installation. Ici, A, B, C et D représentent les périphériques ASA, et H1 et H2 représentent les routeurs IOS.

ASA-A :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.60 255.255.255.0
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 25.1.1.60 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 35.1.1.60 255.255.255.0
```

ASA-B :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 45.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut
```

```
ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 25.1.1.61 255.255.255.0
```

ASA-C :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 55.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 35.1.1.61 255.255.255.0
```

ASA-D :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config) #interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif inside-1
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 45.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif inside-2
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 55.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 65.1.1.60 255.255.255.0
```

H1 :

```
ciscoasa(config)# interface Loopback1
ciscoasa(config-if)# ip address 15.1.1.100 255.255.255.255

ciscoasa(config-if)# interface Loopback2
ciscoasa(config-if)# ip address 15.1.1.101 255.255.255.255

ciscoasa(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.60
```

H2 :

```
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# ip address 65.1.1.100 255.255.255.0

ciscoasa(config-if)# ip route 15.1.1.0 255.255.255.0 65.1.1.60
```

Nous configurerons PBR sur ASA-A pour acheminer le trafic provenant de H1.

ASA-A :

```
ciscoasa(config-if)# access-list pbracl_1 extended permit ip host 15.1.1.100 any

ciscoasa(config-if)# route-map testmap permit 10
ciscoasa(config-if)# match ip address pbracl_1
ciscoasa(config-if)# set ip next-hop 25.1.1.61

ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmap

ciscoasa(config-if)# debug policy-route
```

H1 : envoi d'un message Ping 65.1.1.100 répétition 1 boucle avec retour à la source 1

```
pbr: policy based route lookup called for 15.1.1.100/44397 to 65.1.1.100/0 proto 1 sub_proto
 8 received on interface inside
pbr: First matching rule from ACL(2)
pbr: route map testmap, sequence 10, permit; proceed with policy routing
pbr: evaluating next-hop 25.1.1.61
pbr: policy based routing applied; egress_ifc = outside : next_hop = 25.1.1.61
```

Le paquet est transféré comme prévu en utilisant l'adresse de saut suivant dans la carte de routage.

Lorsqu'un prochain saut est configuré, nous effectuons une recherche dans la table de routage d'entrée pour identifier une route connectée vers le prochain saut configuré et utiliser l'interface correspondante. La table de routage d'entrée pour cet exemple est affichée ici (avec l'entrée de route correspondante mise en surbrillance).

```
in   255.255.255.255 255.255.255.255 identity
in   10.1.1.60       255.255.255.255 identity
in   25.1.1.60       255.255.255.255 identity
in   35.1.1.60       255.255.255.255 identity
in   10.127.46.17    255.255.255.255 identity
in   10.1.1.0        255.255.255.0   inside
in   25.1.1.0        255.255.255.0   outside
in   35.1.1.0        255.255.255.0   dmz
```

Ensuite, configurons ASA-A pour acheminer les paquets H1 de boucle avec retour à la source 2 hors de l'interface DMZ d'ASA-A.

```
ciscoasa(config)# access-list pbracl_2 extended permit ip host 15.1.1.101 any

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address pbracl
ciscoasa(config-route-map)# set ip next-hop 35.1.1.61

ciscoasa(config)# show run route-map
!
```

```
route-map testmap permit 10
  match ip address pbracl_1
  set ip next-hop 25.1.1.61
!
route-map testmap permit 20
  match ip address pbracl_2
  set ip next-hop 35.1.1.61
!
```

H1 : envoi d'un message Ping 65.1.1.100 répétition 1 boucle avec retour à la source 2

Les débogages sont affichés ici :

```
pbr: policy based route lookup called for 15.1.1.101/1234 to 65.1.1.100/1234 proto 6 sub_proto
 0 received on interface inside
pbr: First matching rule from ACL(3)
pbr: route map testmap, sequence 20, permit; proceed with policy routing
pbr: evaluating next-hop 35.1.1.61
pbr: policy based routing applied; egress_ifc = dmz : next_hop = 35.1.1.61
```

et l'entrée de route choisie dans la table de routage d'entrée est affichée ici :

```
in   255.255.255.255 255.255.255.255 identity
 in   10.1.1.60       255.255.255.255 identity
 in   25.1.1.60       255.255.255.255 identity
 in   35.1.1.60       255.255.255.255 identity
 in   10.127.46.17    255.255.255.255 identity
 in   10.1.1.0        255.255.255.0   inside
 in   25.1.1.0        255.255.255.0   outside
 in   35.1.1.0        255.255.255.0   dmz
```

Historique du routage basé sur des politiques

Tableau 37 : Historique des cartes de routage

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Indicateurs de supervision des chemins d'accès dans PBR.	9.18(1)	PBR utilise les mesures pour déterminer le meilleur chemin (interface de sortie) pour transférer le trafic. La supervision des chemins informe périodiquement PBR de l'interface surveillée dont la métrique a été modifiée. PBR récupère les dernières valeurs de métrique pour les interfaces surveillées à partir de la base de données de surveillance des chemins et met à jour le chemin d'accès des données. Commandes nouvelles/modifiées : **clear path-monitoring**, **policy-route**, **show path-monitoring**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage basé sur les politiques	9.4(1)	Le routage basé sur les politiques (PBR) est un mécanisme par lequel le trafic est acheminé par des chemins spécifiques avec une QoS spécifiée à l'aide d'ACL. Les ACL permettent de classer le trafic en fonction du contenu des en-têtes de couche 3 et de couche 4 du paquet. Cette solution permet aux administrateurs de fournir une QoS à un trafic différencié, de répartir le trafic interactif et par lots entre des chemins permanents à faible bande passante et à faible coût et des chemins commutés à bande passante élevée et à coût élevé, et permet aux fournisseurs de services Internet et à d'autres organisations d'acheminer le trafic provenant de divers ensembles d'utilisateurs par le biais de connexions Internet bien définies. Nous avons introduit les commandes suivantes : **set ip next-hop verify-availability**, **set ip next-hop**, **set ip next-hop recursive**, **set interface**, **set ip default next-hop, set default interface**, **set ip df**, **set ip dscp**, **policy-route route-map**, **show policy-route**, **debug policy-route**
Prise en charge d'IPv6 pour le routage basé sur les politiques	9.5(1)	Les adresses IPv6 sont désormais prises en charge pour le routage basé sur les politiques. Nous avons introduit les commandes suivantes : **set ipv6 next-hop**,**set default ipv6-next hop**, **set ipv6 dscp**
Prise en charge de VXLAN pour le routage basé sur les politiques	9.5(1)	Vous pouvez maintenant activer le routage basé sur les politiques sur une interface VNI. Nous n'avons pas modifié de commandes.
Prise en charge du routage basé sur les politiques pour le pare-feu d'identité et Cisco TrustSec	9.5(1)	Vous pouvez configurer le pare-feu d'identité et Cisco TrustSec, puis utiliser les ACL du pare-feu d'identité et Cisco TrustSec dans les cartes de routage basées sur les politiques. Nous n'avons pas modifié de commandes.



CHAPITRE 30

Cartes de routage

Ce chapitre décrit comment configurer et personnaliser les cartes de routage pour l'ASA.

- À propos des cartes de routage, à la page 981
- Lignes directrices relatives aux cartes de routage, à la page 983
- Définir une carte de routage, à la page 983
- Personnaliser une carte de routage, à la page 983
- Exemple de cartes de routage, à la page 986
- Historique des cartes de routage, à la page 986

À propos des cartes de routage

Les cartes de routage sont utilisées lors de la redistribution des routes dans un processus de routage OSPF, RIP, EIGRP ou BGP. Elles sont également utilisées lors de la génération d'une route par défaut dans un processus de routage. Une carte de routage définit les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible.

Les cartes de routage ont de nombreuses caractéristiques en commun avec les listes de contrôle d'accès bien connues. Voici quelques-unes des caractéristiques communes aux deux :

- Il s'agit d'une séquence ordonnée d'instructions individuelles, et chacune a un résultat d'autorisation ou de refus. L'évaluation d'une liste de contrôle d'accès ou d'une carte de routage comprend une analyse de liste, dans un ordre prédéterminé, et une évaluation des critères de chaque énoncé qui correspond. Une analyse de liste est abandonnée une fois que la première correspondance d'instruction est trouvée et qu'une action associée à la correspondance d'instruction est effectuée.
- Ce sont des mécanismes génériques. Les correspondances de critères et l'interprétation des correspondances sont dictées par la façon dont elles sont appliquées et par la fonctionnalité qui les utilise. Une carte de routage appliquée à différentes entités peut être interprétée différemment.

Voici quelques-unes des différences entre les cartes de routage et les listes de contrôle d'accès :

- Les cartes de routage sont plus flexibles que les listes de contrôle d'accès et peuvent vérifier les routages en fonction de critères que les listes de contrôle d'accès ne peuvent pas vérifier. Par exemple, une carte de routage peut vérifier si le type de routage est interne.
- Chaque liste de contrôle d'accès se termine par une instruction de refus implicite, par convention de conception. Si la fin d'une carte de routage est atteinte pendant les tentatives de mise en correspondance, le résultat dépend de l'application spécifique de la carte de routage. Les cartes de routage appliquées à

la *redistribution* se comportent de la même manière que les listes de contrôle d'accès : si la route ne correspond à aucune clause d'une carte de routage, la redistribution de la route est refusée, comme si la carte de routage contient une déclaration de refus à la fin.

Clauses d'autorisation et de refus

Les cartes de routage peuvent avoir des clauses d'autorisation et de refus. La clause deny rejette les correspondances de routage de la redistribution. Vous pouvez utiliser une liste de contrôle d'accès comme critère de correspondance dans la carte de routage. Étant donné que les listes de contrôle d'accès ont également des clauses d'autorisation et de refus, les règles suivantes s'appliquent lorsqu'un paquet correspond à la liste de contrôle d'accès :

- ACL permit + route map permit : les routes sont redistribuées.
- ACL permit + route map deny : les routes ne sont pas redistribuées.
- ACL deny + route map permit or deny : la clause route-map n'est pas mise en correspondance et la prochaine clause route-map est évaluée.

Valeurs de clause de correspondance et de définition

Chaque clause de carte de routage a deux types de valeurs :

- Une valeur de correspondance sélectionne les routages auxquels cette clause doit être appliquée.
- Une valeur définie modifie les renseignements qui seront redistribués dans le protocole cible.

Pour chaque voie de routage qui est redistribuée, le routeur évalue d'abord les critères de correspondance d'une clause de la carte de routage. Si les critères de correspondance sont réussis, la route est redistribuée ou rejetée comme l'exige la clause allow ou deny , et certains de ses attributs peuvent être modifiés par les valeurs définies à partir des commandes set . Si les critères de correspondance échouent, cette clause ne s'applique pas à la voie de routage et le logiciel procède à l'évaluation de la voie de routage en fonction de la clause suivante de la carte de routage. L'analyse de la carte de routage se poursuit jusqu'à ce qu'une clause correspondant à la route soit trouvée ou jusqu'à ce que la fin de la carte de routage soit atteinte.

Une correspondance ou une valeur définie dans chaque clause peut être manquée ou répétée plusieurs fois, si l'une de ces conditions est remplie :

- Si plusieurs entrées de correspondance sont présentes dans une clause, elles doivent toutes réussir pour une route donnée afin que cette route corresponde à la clause (c'est-à-dire que l'algorithme AND logique est appliqué pour plusieurs commandes de correspondance).
- Si une entrée de correspondance fait référence à plusieurs objets dans une seule entrée, l'un ou l'autre doit correspondre (l'algorithme OU logique est appliqué).
- En l'absence d'entrée de correspondance, toutes les routes correspondent à la clause.
- Si une entrée d'ensemble n'est pas présente dans une clause d'autorisation de carte de routage, la route est redistribuée sans modification de ses attributs actuels.

Remarque Ne configurez pas d'entrée d'ensemble dans une clause de refus de carte de routage, car la clause de refus interdit la redistribution de routage : il n'y a aucun renseignement à modifier.

Une clause de carte de routage sans entrée de correspondance ou d'ensemble effectue une action. Une clause d'autorisation vide permet une redistribution des routes restantes sans modification. Une clause de refus vide ne permet pas une redistribution d'autres routes (il s'agit de l'action par défaut si une carte de routage est complètement analysée, mais qu'aucune correspondance explicite n'est trouvée).

Lignes directrices relatives aux cartes de routage

Mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Directives supplémentaires

Les cartes de routage ne prennent pas en charge les ACL qui incluent un utilisateur, un groupe d'utilisateurs ou des objets de nom de domaine complet.

Définir une carte de routage

Vous devez définir une carte de routage lorsque vous précisez les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible.

Procédure

Créez l'entrée de carte de routage :

route-map *nom* {**permis** | **refuser**} [*numéro_séquence*]

Exemple :

```
ciscoasa(config)# route-map name {permit} [12]
```

Les entrées de carte de routage sont lues dans l'ordre. Vous pouvez identifier l'ordre à l'aide de l'argument *sequence_number* ou l'ASA utilise l'ordre dans lequel vous ajoutez les entrées de la carte de routage.

Personnaliser une carte de routage

Cette section décrit comment personnaliser la carte de routage.

Définir une route pour correspondre à une adresse de destination spécifique

Procédure

Étape 1 Créez l'entrée de carte de routage :

route-map *nom* {**permis** | **refuser**} [*numéro_séquence*]

Exemple :

```
ciscoasa(config)# route-map name {permit} [12]
```

Les entrées de carte de routage sont lues dans l'ordre. Vous pouvez identifier l'ordre à l'aide de l'argument *sequence_number*, ou l'ASA utilise l'ordre dans lequel vous ajoutez les entrées de la carte de routage.

Étape 2 Faites correspondre toutes les routes dont le réseau de destination correspond à une ACL ou une liste de préfixes standard :

match ip address {*acl_id* [*acl_id*] [...] | **prefix-list** *prefix_list_id* [*prefix_list_id*] [...]}

Exemple :

```
ciscoasa(config-route-map)# match ip address acl1 acl2 acl3
```

Si vous spécifiez plusieurs ACL ou listes de préfixes, la route peut correspondre à n'importe quelle ACL ou liste de préfixes.

Étape 3 Faites correspondre toutes les routes qui ont une mesure spécifiée :

match metric *metric_value*

Exemple :

```
ciscoasa(config-route-map)# match metric 200
```

Les valeurs *metric_value* peuvent être comprises entre 0 et 4294967295.

Étape 4 Faites correspondre toutes les routes qui ont une adresse de routeur de saut suivant correspondant à une ACL standard :

match ip next-hop *acl_id* [*acl_id*] [...]

Exemple :

```
ciscoasa(config-route-map)# match ip next-hop acl2
```

Si vous spécifiez plusieurs ACL, la route peut correspondre à n'importe quelle ACL.

Étape 5 Faites correspondre toutes les routes avec l'interface de saut suivant spécifiée :

match interface *if_name*

Exemple :

```
ciscoasa(config-route-map)# match interface if_name
```

Si vous spécifiez plusieurs interfaces, la route peut correspondre à l'une ou l'autre des interfaces.

Étape 6 Faites correspondre toutes les routes qui ont été annoncées par les routeurs correspondant à une ACL standard :

match ip route-source *acl_id* [*acl_id*] [...]

Exemple :

```
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

Si vous spécifiez plusieurs ACL, la route peut correspondre à n'importe quelle ACL.

Étape 7 Faites correspondre le type de route :

match route-type {**internal** | **external** [**type-1** | **type-2**]}

Configurer les valeurs de mesure pour une action de routage

Si une route correspond aux commandes **match**, les commandes **set** suivantes déterminent l'action à effectuer sur la route avant de la redistribuer.

Pour configurer la valeur de mesure d'une action de routage, procédez comme suit :

Procédure

Étape 1 Créez l'entrée de carte de routage :

route-map *nom* {**permis** | **refuser**} [*numéro_séquence*]

Exemple :

```
ciscoasa(config)# route-map name {permit} [12]
```

Les entrées de carte de routage sont lues dans l'ordre. Vous pouvez identifier l'ordre à l'aide de l'argument *sequence_number* ou l'ASA utilise l'ordre dans lequel vous ajoutez les entrées de la carte de routage.

Étape 2 Définissez la valeur de la mesure de la carte de routage :

set metric *metric_value*

Exemple :

```
ciscoasa(config-route-map)# set metric 200
```

L'argument *metric_value* peut aller de 0 à 294967295.

Étape 3 Définissez le type de mesure pour la carte de routage :

set metric-type {**type-1** | **type-2**}

Exemple :

```
ciscoasa(config-route-map)# set metric-type type-2
```

L'argument *metric-type* peut être type-1 ou type-2.

Exemple de cartes de routage

L'exemple suivant montre comment redistribuer les routes avec un nombre de sauts égal à 1 dans OSPF.

L'ASA redistribue ces routes en tant que LSA externes avec une mesure de 5 et un type de mesure de type 1.

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

L'exemple suivant montre comment redistribuer la route statique 10.1.1.0 dans le processus EIGRP 1 avec la valeur de la mesure configurée :

```
ciscoasa(config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config-router)# redistribute static metric 250 250 1 1 1 route-map mymap2
```

Historique des cartes de routage

Tableau 38 : Historique des fonctionnalités pour les cartes de routage

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Cartes de routage	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit la commande suivante : **route-map**.
Prise en charge améliorée pour les cartes de routage statiques et dynamiques	8.0(2)	Une prise en charge améliorée des cartes de routage dynamiques et statiques a été ajoutée.
Prise en charge du basculement dynamique des protocoles de routage dynamique (EIGRP, OSPF et RIP) et du débogage des opérations générales liées au routage	v 8.4(1)	Nous avons introduit les commandes suivantes : **debug route**, **show debug route**. Nous avons modifié la commande suivante : **show route**.
Routage dynamique en mode de contexte multiple	9.0(1)	Les cartes de routage sont prises en charge en mode de contexte multiple.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge BGP	9.2(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les commandes suivantes : **router bgp**
Prise en charge d'IPv6 pour la règle de préfixe	9.3.2	Nous avons introduit cette fonctionnalité.



CHAPITRE 31

Routage par détection de transfert bidirectionnel (BFD)

Ce chapitre décrit comment configurer l'ASA pour utiliser le protocole de routage par détection de transfert bidirectionnel (BFD).

- À propos du routage BFD, à la page 989
- Directives pour le routage BFD, à la page 993
- Configurer BFD, à la page 993
- Supervision BFD, à la page 997
- Historique du routage BFD, à la page 998

À propos du routage BFD

BFD est un protocole de détection conçu pour fournir des temps de détection de défaillance du chemin d'acheminement rapides pour tous les types de médias, encapsulations, topologies et protocoles de routage. BFD fonctionne en mode point à point de monodiffusion en plus de tout protocole de données transféré entre deux systèmes. Les paquets sont transportés dans la charge utile du protocole d'encapsulation approprié pour le support et le réseau.

BFD fournit une méthode de détection des défaillances cohérente pour les administrateurs réseau en plus de la détection des défaillances du chemin de transfert rapide. Comme l'administrateur réseau peut utiliser BFD pour détecter les défaillances du chemin de transfert à un débit uniforme, plutôt que pour les débits variables, pour les différents mécanismes Hello du protocole de routage, le profilage et la planification du réseau sont plus faciles et le temps de reconversion est uniforme et prévisionnel.

Mode asynchrone BFD et fonction d'écho

La BFD peut fonctionner en mode asynchrone avec ou sans la fonction d'écho activée.

Mode asynchrone

En mode asynchrone, les systèmes envoient périodiquement des paquets de contrôle de la BFD l'un à l'autre, et si un certain nombre de paquets de la ligne ne sont pas reçus par l'autre système, la session est déclarée inactive. Le mode asynchrone pur (sans la fonction d'écho) est utile, car il nécessite deux fois moins de paquets pour atteindre un temps de détection particulier.

Fonction d'écho de la BFD

La fonction d'écho de la BFD envoie des paquets d'écho du moteur de transfert au voisin BFD à saut unique directement connecté. Les paquets écho sont envoyés par le moteur de transfert et redirigés le long du même chemin pour effectuer la détection. La session BFD à l'autre extrémité ne participe pas au transfert réel des paquets écho. Comme la fonction d'écho et le moteur de transfert sont responsables du processus de détection, le nombre de paquets de contrôle de la BFD qui sont envoyés entre les voisins de la BFD est réduit. Puisque le moteur de transfert teste le chemin de transfert sur le système voisin distant sans interagir avec le système distant, la variation du délai entre les paquets est augmentée. Cela se traduit par des délais de détection des défaillances plus rapides.

Lorsque la fonction d'écho est activée, la BFD peut utiliser la minuterie lente pour retarder la session asynchrone et réduire le nombre de paquets de contrôle de BFD envoyés entre les voisins de BFD, ce qui réduit le surdébit de traitement tout en permettant une détection plus rapide des défaillances.

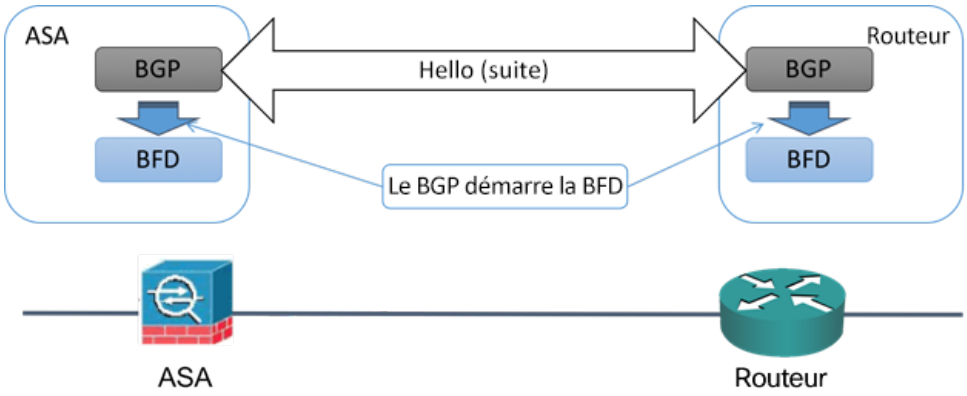
Remarque La fonction d'écho n'est pas prise en charge pour les voisins BFD à multisaut IPv4 ou à saut unique IPv6.

Vous pouvez activer la BFD au niveau de l'interface et du protocole de routage. Vous devez configurer la BFD sur les deux systèmes (homologues BFD). Après avoir activé la BFD sur les interfaces et au niveau du routeur pour les protocoles de routage appropriés, une session BFD est créée, les minuteries de la BFD sont négociées et les homologues de la BFD commencent à s'envoyer des paquets de contrôle de la BFD au niveau négocié.

Établissement de la session BFD

L'exemple suivant montre l'ASA et un routeur voisin exécutant le protocole de passerelle frontière (BGP). Au moment où les deux appareils démarrent, aucune session BFD n'est établie entre eux.

Illustration 68 : Session BFD établie



Une fois que le protocole BGP a identifié son voisin BGP, il démarre le processus BFD avec l'adresse IP du voisin. La BFD ne détecte pas ses homologues de manière dynamique. Elle s'appuie sur les protocoles de routage configurés pour lui indiquer quelles adresses IP utiliser et quelles relations d'homologues former.

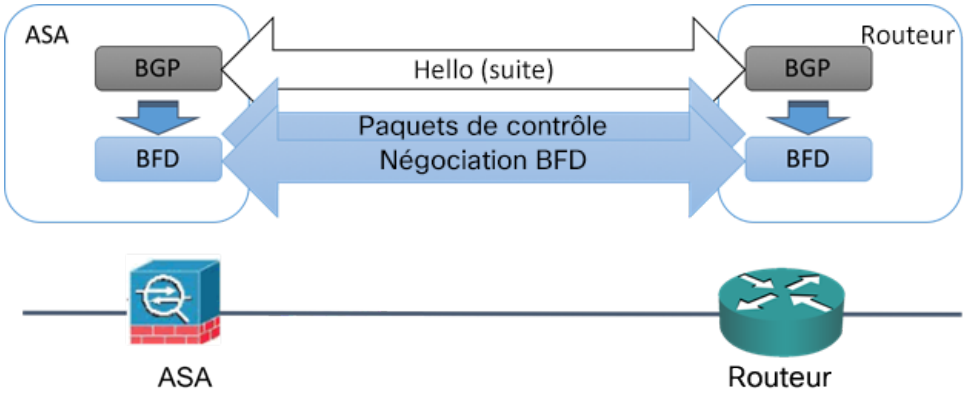
La BFD sur le routeur et la BFD sur l'ASA forment un paquet de contrôle de BFD et commencent à s'envoyer des paquets à un intervalle d'une seconde jusqu'à ce que la session BFD soit établie. Les paquets de contrôle initiaux de l'un ou l'autre des systèmes sont très similaires. Par exemple, les bits Vers, Diag, H, D, P et F sont

tous définis sur zéro et l'état est défini sur Down (En panne). Le champ My Discriminator (Mon discriminateur) est défini sur une valeur unique sur le périphérique de transmission. Le champ Your Discriminator (Votre discriminateur) est défini sur zéro, car la session BFD n'a pas encore été établie. Les minuteries TX et RX sont définies aux valeurs trouvées dans la configuration de l'appareil.

Une fois que le périphérique BFD distant a reçu un paquet de contrôle de BFD pendant la phase d'ouverture de session, il copie la valeur du champ My Discriminator (Mon discriminateur) dans son propre champ Your Discriminator (Votre discriminateur) et la transition de l'état Down (En panne) à l'état Init (Initialisation), puis finalement à l'état Up (Opérationnel) se produit. Une fois que les deux systèmes ont vu leurs propres discriminateurs dans les paquets de contrôle de l'autre, la session est officiellement établie.

L'illustration suivante montre la connexion BFD établie.

Illustration 69 : BGP sans session BFD établie



Négociation de la minuterie BFD

Les appareils BFD doivent négocier les minuteries BFD pour contrôler et synchroniser le débit d'envoi des paquets de contrôle BFD. Un périphérique doit s'assurer des éléments suivants avant de pouvoir négocier une minuterie BFD :

- Que son appareil homologue a vu le paquet contenant les minuteries proposées par le périphérique local
- Qu'il n'envoie jamais de paquets de contrôle BFD plus rapidement que l'homologue n'est configuré pour les recevoir
- Que l'homologue n'envoie jamais de paquets de contrôle BFD plus rapidement que le système local n'est configuré pour les recevoir

Les paramètres du champ Your Discriminator (Votre discriminateur) et du bit H suffisent pour indiquer au périphérique local que le périphérique distant a vu ses paquets lors de l'échange initial de la minuterie. Après avoir reçu un paquet de contrôle BFD, chaque système prend l'intervalle RX minimum requis et le compare à son propre intervalle TX minimum souhaité, puis prend la plus grande (la plus lente) des deux valeurs et l'utilise comme débit de transmission pour ses paquets BFD. Le plus lent des deux systèmes détermine le débit de transmission.

Lorsque ces minuteries ont été négociées, elles peuvent être renégociées à tout moment pendant la session sans entraîner de réinitialisation de session. Le périphérique qui modifie ses minuteries règle le bit P sur tous les paquets de contrôle BFD suivants jusqu'à ce qu'il reçoive un paquet de contrôle BFD avec le bit F défini pour le système distant. Cet échange de bits permet d'éviter la perte de paquets pendant le transit.

Remarque Le réglage du bit F par le système distant ne signifie pas qu'il accepte les nouvelles minuteries proposées. Il indique que le système distant a vu les paquets dans lesquels les minuteries ont été modifiées.

Détection de défaillance BFD

Une fois la session BFD et les minuteries négociées, les homologues BFD s'envoient des paquets de contrôle BFD à l'intervalle négocié. Ces paquets de contrôle agissent comme une pulsation très similaire au protocole IGP Hello, sauf que le débit est plus accéléré.

Tant que chaque homologue de la BFD reçoit un paquet de contrôle de la BFD dans le cadre de l'intervalle de détection configuré (intervalle RX minimal requis), la session de la BFD reste active et tout protocole de routage associé à la BFD conserve ses contiguïtés. Si un homologue BFD ne reçoit pas de paquet de contrôle dans cet intervalle, il informe tous les clients participant à cette session BFD de la défaillance. Le protocole de routage détermine la réponse appropriée à ces renseignements. La réponse typique est de mettre fin à la session d'appairage du protocole de routage et de reconverger, et ainsi de contourner un homologue défaillant.

Chaque fois qu'un homologue BFD reçoit avec succès un paquet de contrôle BFD dans une session BFD, la minuterie de détection pour cette session est réinitialisée à zéro. La détection des défaillances dépend donc des paquets reçus et NON de la dernière transmission d'un paquet par le récepteur.

Scénarios de déploiement BFD

Les éléments suivants décrivent le fonctionnement de la BFD dans ces scénarios spécifiques.

Basculement

Dans un scénario de basculement, des sessions BFD sont établies et maintenues entre l'unité active et l'unité voisine. Les unités en veille ne maintiennent aucune session BFD avec leurs voisins. Lors d'un basculement, la nouvelle unité active doit initier l'établissement d'une session avec le voisin, car les renseignements sur la session ne sont pas synchronisés entre les unités actives et de secours.

Pour un scénario de redémarrage progressif/NSF, le client (BGP IPv4/IPv6) est chargé d'informer son voisin de l'événement. Lorsque le voisin reçoit les renseignements, il conserve la table RIB jusqu'à ce que le basculement soit terminé. Pendant le basculement, les sessions BFD et BGP sont inactives sur l'appareil. Une fois le basculement terminé, une nouvelle session BFD entre les voisins est établie lorsque la session BGP est lancée.

EtherChannel étendu et grappe L2

Dans un scénario de grappe EtherChannel étendu, la session BFD est établie et maintenue entre l'unité principale et son voisin. Les unités subordonnées ne maintiennent aucune session BFD avec leurs voisins. Si un paquet BFD est acheminé vers l'unité subordonnée en raison de l'équilibrage de charges sur le commutateur, l'unité subordonnée doit transférer ce paquet à l'unité principale par la liaison de grappe. Lorsqu'un basculement de grappe se produit, la nouvelle unité principale doit initier l'établissement d'une session avec le voisin, car les renseignements sur la session ne sont pas synchronisés entre les unités principale et subordonnée.

Mode d'interface individuelle et grappe L3

Dans un scénario de grappe en mode d'interface individuelle, les unités individuelles maintiennent leurs sessions BFD avec leurs voisins.

Directives pour le routage BFD

Directives relatives au mode contextuel

Pris en charge en modes de contexte unique et multiple.

Directives sur le mode pare-feu

Pris en charge en mode de pare-feu routé; prise en charge des modes autonome, de basculement et de grappe. La BFD n'est pas prise en charge sur les interfaces de basculement. Dans la mise en grappe, cette fonctionnalité n'est prise en charge que sur l'unité principale. La BFD n'est pas prise en charge en mode transparent.

Directives IPv6

Le mode Echo n'est pas pris en charge pour IPv6.

Directives supplémentaires

Les protocoles BGP IPv4et BGP IPv6 sont pris en charge.

Les protocoles OSPFv2, OSPFv3, IS-IS et EIGRP ne sont pas pris en charge.

La BFD pour les routes statiques n'est pas pris en charge.

La BFD de transfert et de tunnel n'est pas prise en charge.

Remarque Pour un routage optimal, ne configurez pas la BFD lorsque le redémarrage progressif du BGP pour NSF est configuré sur le périphérique.

Configurer BFD

Cette section décrit comment activer et configurer le processus de routage BFD sur votre système.

Procédure

Étape 1 Créer le modèle BFD, à la page 993.

Étape 2 Configurer les interfaces BFD, à la page 995.

Étape 3 Configurer les cartes BFD, à la page 997.

Créer le modèle BFD

Cette section décrit les étapes requises pour créer un modèle de BFD et passer en mode de configuration de la BFD.

Le modèle BFD spécifie un ensemble de valeurs d'intervalle BFD. Les valeurs d'intervalle BFD configurées dans le modèle BFD ne sont pas spécifiques à une interface unique. Vous pouvez également configurer l'authentification pour les sessions à saut unique et à sauts multiples. Vous pouvez activer Echo sur un seul saut uniquement.

Procédure

Étape 1 Activez la BFD comme protocole de routage sur l'ASA en créant le modèle de BFD, à saut unique ou à multisaut :

bfd-template [single-hop | multi-hop] *template_name*

Exemple :

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)#
```

- **single-hop** : spécifie un modèle de BFD à saut unique.
- **multi-hop** : spécifie un modèle de BFD à multisaut.
- *template-name* : spécifie le nom du modèle. Le nom du modèle ne peut pas contenir d'espaces.

La commande **bfd-template** vous permet de créer le modèle de BFD et de passer en mode de configuration de la BFD.

Étape 2 (Facultatif) Configurez Echo sur un modèle de BFD à saut unique :

bfd-template single-hop *template_name*

Exemple :

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa (config-bfd)# echo
```

Vous pouvez activer le mode Echo sur un modèle à saut unique. L'écho de la BFD n'est pas pris en charge pour les sessions BFD IPv6.

Étape 3 Configurez les intervalles dans le modèle de BFD :

interval [**both** *milliseconds* | **microseconds {both | min-tx}** *microseconds* | **min-tx** *milliseconds*

Exemple :

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# interval both 50
```

- **both** : capacité minimale d'intervalle de transmission et de réception.
- *milliseconds* : intervalle en millisecondes. La plage se situe entre 50 et 999.
- **microseconds** : spécifie l'intervalle BFD en microsecondes pour **both** et **min-tx**.
- *microseconds* : la plage se situe entre 50 000 et 999 000.
- **min-tx** : capacité minimale d'intervalle de transmission.

Les valeurs d'intervalle BFD spécifiées dans le modèle de BFD ne sont pas spécifiques à une interface unique. Vous pouvez appliquer des modèles de BFD individuels par interface. Consultez Configurer les interfaces BFD, à la page 995.

Étape 4 Configurez l'authentification dans le modèle de BFD :

authentication {md5 | meticulous-mds | meticulous-sha-1 | sha-1} [0|8] *word* **key-id** *id*

Exemple :

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

- **authentication** : spécifie le type d'authentification.
- **md5** : authentification Message Digest 5 (MD5).
- **meticulous-md5** : authentification MD5 à clé précise.
- **meticulous-sha-1** : authentification SHA-1 à clé précise.
- **sha-1** : authentification SHA-1 à clé.
- **0|8** : 0 spécifie qu'un mot de passe NON CHIFFRÉ suivra. Le numéro 8 indique qu'un mot de passe CHIFFRÉ suivra.
- *word* : le mot de passe (clé) de la BFD, qui est un mot de passe/une clé à un chiffre de 29 caractères maximum. Les mots de passe commençant par un chiffre suivi d'un espace blanc ne sont pas pris en charge. Par exemple, « 0 pass » et « 1 » ne sont pas valides.
- **key-id** : ID de la clé d'authentification.
- *id* : ID de clé partagée qui correspond à la valeur de clé. La valeur est comprise entre 0 et 255 caractères.

Vous pouvez configurer l'authentification dans des modèles à saut unique et multisaut. Nous vous conseillons de configurer l'authentification pour renforcer la sécurité. Vous devez configurer l'authentification sur chaque paire source-destination BFD et les paramètres d'authentification doivent correspondre sur les deux périphériques.

Configurer les interfaces BFD

Vous pouvez lier un modèle BFD à une interface, configurer les paramètres de session BFD de référence par interface et activer le mode écho par interface.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
```

```
ciscoasa(config-if)#
```

Étape 2 Appliquez un modèle BFD à une interface :

bfd template *template-name*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# bfd template TEMPLATE1
```

Même si vous n'avez pas créé de modèle à l'aide de la commande **bfd-template**, vous pouvez configurer le nom du modèle sous une interface, mais le modèle est considéré comme non valide tant que vous ne l'avez pas défini. Vous n'avez pas à reconfigurer le nom du modèle. Il devient automatiquement valide.

Étape 3 Configurez les paramètres de session BFD :

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-router)# bfd interval 200 min_rx 200 multiplier 3
```

- **interval** *milliseconds* : spécifie le débit auquel les paquets de contrôle BFD sont envoyés aux homologues BFD. La plage va de 50 à 999 millisecondes.
- **min_rx** *milliseconds* : spécifie le débit auquel les paquets de contrôle BFD doivent être reçus des homologues BFD. La plage va de 50 à 999 millisecondes.
- **multiplier** *multiplier-value* : indique le nombre de paquets de contrôle BFD consécutifs qui doivent être manqués par un homologue BFD avant que la BFD ne déclare que l'homologue n'est pas disponible et que l'homologue BFD de couche 3 soit informé de la défaillance. La valeur doit être comprise entre 3 et 50.

Étape 4 Activez le mode d'écho de la BFD sur une interface :

bfd echo

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(if)# bfd echo
```

Le mode écho est activé par défaut, mais n'est pas pris en charge dans les sessions IPv6 de la BFD. Lorsque le mode écho est activé, les valeurs minimum du niveau de transmission écho et de l'intervalle de transmission requis sont tirées de la configuration **bfd interval** *milliseconds* **min_rx** *milliseconds*.

Remarque
Avant d'utiliser le mode d'écho de la BFD, vous devez désactiver les messages de redirection ICMP à l'aide de la commande **no ip redirects**. Cela permet d'éviter une utilisation élevée du processeur.

Configurer les cartes BFD

Vous pouvez créer une carte BFD contenant des destinations que vous pouvez associer à un modèle multisaut. Vous devez disposer d'un modèle BFD multisaut déjà configuré.

Procédure

Étape 1 Créez un modèle BFD multisaut. Reportez-vous à Créer le modèle BFD, à la page 993 pour connaître la procédure.

Étape 2 Associez le modèle BFD multisaut à une carte de destinations :

bfd map {ipv4 | ipv6} *destination/cdir source/cdire template-name*

Exemple :

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
ciscoasa(config-bfd)#
```

- **ipv4** : configure une adresse IPv4.
- **ipv6** : configure une adresse IPv6.
- *destination/cdir* : spécifie le préfixe et la longueur du préfixe de destination. Le format est A.B.C.D/<0-32>.
- *source/cdir* : spécifie le préfixe et la longueur du préfixe de destination. Le format est X:X:X;X::X/<0-128>.
- *template-name* : spécifie le nom du modèle multisaut associé à cette carte BFD.

Étape 3 (Facultatif) Configurez la valeur des minuteries lentes de la BFD :

bfd slow-timers [*milliseconds*]

Exemple :

```
ciscoasa(config)# bfd slow-timers 14000
ciscoasa(config-bfd)#
```

milliseconds : (Facultatif) La valeur des minuteries lentes de la BFD. La plage se situe entre 1 000 et 30 000. La valeur par défaut est de 1 000.

Supervision BFD

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage BFD. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande.

Pour superviser ou désactiver diverses statistiques de routage BFD, saisissez l'une des commandes suivantes :

- **show bfd neighbors**

  Affiche une liste ligne par ligne des contiguïtés BFD existantes.

- **show bfd summary**

  Affiche les renseignements de base sur la BFD, les clients BFD ou les sessions BFD.

- **show bfd drops**

  Affiche le nombre de paquets abandonnés dans la BFD.

- **show bfd map**

  Affiche les cartes BFD configurées.

- **show running-config bfd**

  Affiche la carte BFD et d'autres configurations liées à la BFD.

- **show running-config bfd-template**

  Affiche les configurations liées au modèle BFD.

Historique du routage BFD

Tableau 39 : Historique des fonctionnalités du routage BFD

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du routage BFD	9.6(2)	L'ASA prend désormais en charge le protocole de routage BFD. Une prise en charge a été ajoutée pour la configuration des modèles, des interfaces et des cartes BFD. La prise en charge du protocole de routage BGP pour utiliser BFD a également été ajoutée. Nous avons ajouté les commandes suivantes : **bfd echo, bfd interval, bfd map, bfd slow-timers, bfd-template, clear bfd counters, clear conf bfd, neighbor fall-over bfd, show bfd drops, show bfd map, show bfd neighbors, show bfd summary, show running-config bfd**



CHAPITRE 32

BGP

Ce chapitre décrit comment configurer l'ASA pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de passerelle frontière (BGP).

- À propos de BGP, à la page 999
- Lignes directrices BGP, à la page 1003
- Configurer le protocole BGP, à la page 1003
- Supervision BGP, à la page 1034
- Exemple de BGP, à la page 1037
- Historique de BGP, à la page 1039

À propos de BGP

BGP est un protocole de routage de systèmes inter et intra autonomes. Un système autonome est un réseau ou un groupe de réseaux soumis à une administration et à des politiques de routage communes. BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les fournisseurs de services Internet (ISP).

Quand utiliser BGP

Les réseaux des clients, comme les universitaires et les entreprises, emploient généralement un protocole IGP (Interior Gateway Protocol) comme OSPF pour l'échange d'informations de routage au sein de leurs réseaux. Les clients se connectent aux fournisseurs de services Internet, et les fournisseurs de services Internet utilisent BGP pour échanger les routes du client et des fournisseurs de services Internet. Lorsque BGP est utilisé entre des systèmes autonomes (AS), le protocole est appelé BGP externe (EBGP). Si un fournisseur de services utilise BGP pour échanger des routages au sein d'un système autonome, le protocole est appelé BGP intérieur (IBGP).

BGP peut également être utilisé pour acheminer des informations de routage pour le préfixe IPv6 sur les réseaux IPv6.

Remarque Lorsqu'un périphérique BGPv6 rejoint la grappe, il génère un traçage logiciel lorsque le niveau de journalisation 7 est activé.

Modifications apportées à la table de routage

Les voisins BGP échangent des informations de routage complètes lors de la connexion TCP entre voisins est établie pour la première fois. Lorsque des modifications de la table de routage sont détectées, les routeurs BGP envoient à leurs voisins uniquement les routes qui ont été modifiées. Les routeurs BGP n'envoient pas de mises à jour de routage périodiques et les mises à jour de routage BGP n'annoncent que le chemin optimale vers un réseau de destination.



Remarque La détection de boucle AS se fait en analysant le chemin AS complet (comme spécifié dans l'attribut AS_PATH) et en vérifiant que le numéro de système autonome du système local ne figure pas dans le chemin AS. Par défaut, EBGP annonce les routes apprises au même homologue pour éviter des cycles de CPU supplémentaires sur la périphérique lors des vérifications de boucle et des retards dans les tâches de mise à jour sortantes existantes.

Les routes apprises via BGP ont des propriétés utilisées pour déterminer la meilleure route vers une destination, lorsque plusieurs chemins existent vers une destination particulière. Ces propriétés sont appelées attributs BGP et sont utilisées dans le processus de sélection de routage :

- Pondération : il s'agit d'un attribut défini par Cisco qui est local à un routeur. L'attribut de pondération n'est pas annoncé aux routeurs voisins. Si le routeur détecte l'existence de plusieurs routes vers la même destination, la route ayant la pondération la plus élevée est préférée.
- Préférence locale : L'attribut de préférence locale est utilisé pour sélectionner un point de sortie du système autonome local. Contrairement à l'attribut de pondération, l'attribut de préférence locale se propage dans tout le système autonome local. S'il y a plusieurs points de sortie du système autonome, le point de sortie avec l'attribut de préférence locale le plus élevé est utilisé comme point de sortie pour une route spécifique.
- Identifiant multi-sortie : L'attribut de métrique ou de discrimination multi-sortie (MED) est utilisé comme suggestions à un système autonome externe concernant la voie de routage préférée dans le système autonome qui annonce la métrique. Il s'agit d'une suggestions, car le système autonome externe qui reçoit les MED peut également utiliser d'autres attributs de BGP pour la sélection de route. La route avec la métrique MED la plus basse est préférée.
- Origine : l'attribut d'origine indique comment BGP a appris l'existence d'une route particulière. L'attribut d'origine peut avoir l'une des trois valeurs possibles et est utilisé dans la sélection de la route.
  - IGP : la voie de routage est intérieure au système autonome d'origine. Cette valeur est définie lorsque la commande de configuration du routeur network est utilisée pour injecter la voie de routage dans BGP.
  - EGP : le routage est appris par le protocole EBGP (Exterior Border Gateway Protocol).
  - Incomplet : l'origine de la route est inconnue ou apprise d'une autre manière. Une origine incomplète se produit lorsqu'une route est redistribuée dans BGP.
- AS_path : lorsqu'une déclaration de route passe par un système autonome, le numéro de système autonome est ajouté à une liste ordonnée de numéros de système autonome que l'annonce de route a traversés. Seule la voie de routage avec la liste AS_path la plus courte est installée dans la table de routage IP.
- Saut suivant : l'attribut de saut suivant EBGP est l'adresse IP utilisée pour atteindre le routeur publicitaire. Pour les homologues EBGP, l'adresse de saut suivant est l'adresse IP de la connexion entre les

homologues. Pour IBGP, l'adresse du prochain saut EBGP est acheminée dans le système autonome local. Cependant, lorsque le saut suivant se trouve dans le même sous-réseau que l'adresse d'appairage de l'homologue eBGP, le saut suivant n'est pas modifié. Ce comportement est appelé saut suivant du tiers.

Utilisez la commande **next-hop-self** lors de la redistribution des routes annoncées par VPN vers les homologues iBGP pour vous assurer que les routes sont redistribuées avec l'adresse IP du prochain saut appropriée.

- Community (communauté) : L'attribut Community permet de regrouper des destinations, appelées communautés, auxquelles les décisions de routage (telles que l'acceptation, les préférences et la redistribution) peuvent être appliquées. Des cartes de routage sont utilisées pour définir l'attribut de communauté. Les attributs de communauté prédéfinis sont les suivants :
  - no-export : n'annonce pas cette voie de routage aux homologues EBGP.
  - no-advertise : n'annonce cette voie de routage à aucun homologue.
  - Internet : annonce cette route à la communauté Internet; tous les routeurs du réseau lui appartiennent.

Sélection du chemin BGP

BGP peut recevoir plusieurs annonces pour la même route provenant de différentes sources. BGP sélectionne un seul chemin comme meilleur chemin. Lorsque ce chemin est sélectionné, BGP le met dans la table de routage IP et propage le chemin à ses voisins. BGP utilise les critères suivants, dans l'ordre présenté, pour sélectionner un chemin pour une destination :

- Si le chemin précise un saut suivant inaccessible, supprimez la mise à jour.
- Privilégiez le chemin avec la pondération la plus élevée.
- Si les pondérations sont identiques, préférez le chemin avec la préférence locale la plus élevée.
- Si les préférences locales sont les mêmes, le chemin préféré est celui qui a été créé par le protocole BGP exécuté sur ce routeur.
- Si aucune voie de routage n'a été créée, privilégiez la voie de routage qui a le chemin AS_path le plus court.
- Si tous les chemins ont la même longueur AS_path, privilégiez le chemin avec le type d'origine le plus bas (où IGP est inférieur à EGP et EGP est inférieur à incomplet).
- Si les codes d'origine sont les mêmes, privilégiez le chemin avec l'attribut MED le plus bas.
- Si les chemins ont la même MED, privilégiez le chemin externe au chemin interne.
- Si les chemins sont toujours les mêmes, privilégiez le chemin par le voisin IGP le plus proche.
- Déterminez si plusieurs chemins d'accès nécessitent l'installation dans la table de routage pour Chemins multiples BGP, à la page 1002.
- Si les deux chemins sont externes, privilégiez le chemin qui a été reçu en premier (le plus ancien).
- Privilégiez le chemin avec l'adresse IP la plus basse, comme spécifié par l'ID du routeur BGP.
- Si l'ID de l'expéditeur ou du routeur est le même pour plusieurs chemins, privilégiez le chemin avec la longueur minimale de la liste de grappes.

- Privilégiez le chemin qui provient de l’adresse du voisin le plus bas.

Chemins multiples BGP

Les chemins BGP multiples permettent l’installation dans la table de routage IP de plusieurs chemins BGP à coût égal vers le même préfixe de destination. Le trafic vers le préfixe de destination est ensuite partagé sur tous les chemins installés.

Ces chemins sont installés dans le tableau avec le meilleur chemin pour le partage de la charge. Les chemins multiples de BGP n’affectent pas la sélection du meilleur chemin. Par exemple, un routeur désigne toujours l’un des chemins comme le meilleur chemin, selon l’algorithme, et annonce ce meilleur chemin à ses homologues de BGP.

Pour être candidats aux chemins multiples, les chemins vers la même destination doivent avoir ces caractéristiques égales aux caractéristiques du meilleur chemin :

- Poids
- Préférence locale
- Longueur du chemin d'accès AS
- Code d’origine
- Sélecteur de sorties multiples (MED)
- L’une des suivantes :
  - Le système autonome ou sous-système autonome voisin (avant l’ajout des chemins multiples de BGP)
  - AS-PATH (après l’ajout des chemins multiples de BGP)

Certaines fonctionnalités de chemins multiples de BGP appliquent des exigences supplémentaires aux candidats aux chemins multiples :

- Le chemin doit être appris d’un voisin externe ou d’un voisin externe à la confédération (eBGP).
- La métrique IGP au saut suivant de BGP doit être égale à la métrique IGP du meilleur chemin.

Voici les exigences supplémentaires pour les candidats aux chemins multiples de BGP interne (iBGP) :

- Le chemin doit être appris d’un voisin interne (iBGP).
- La métrique IGP jusqu’au saut suivant de BGP doit être égale à la métrique du meilleur chemin IGP, sauf si le routeur est configuré pour les chemins multiples iBGP à coût inégal.

BGP insère jusqu’à *n* derniers chemins reçus de candidats aux chemins multiples dans la table de routage IP, *n* étant le nombre de routes à installer dans la table de routage, comme spécifié lorsque vous configurez BGP multi-chemins. La valeur par défaut, lorsque les chemins multiples est désactivé, est 1.

Pour l’équilibrage de charge à coût inégal, vous pouvez également utiliser la bande passante du lien BGP.



Remarque Le prochain-saut-self équivalent est effectué sur le meilleur chemin sélectionné parmi les chemins multiples eBGP avant qu’il ne soit transmis aux homologues internes.

Lignes directrices BGP

Directives relatives au mode contextuel

- Pris en charge en mode contexte unique et multiple.
- Un seul numéro du système autonome (AS) est pris en charge pour tous les contextes.

Directives sur le mode pare-feu

Le mode pare-feu transparent n'est pas pris en charge. BGP est pris en charge uniquement en mode routé.

Directives IPv6

Prend en charge IPv6.

Directives supplémentaires

- Le système n'ajoute pas d'entrée de routage pour l'adresse IP reçue sur PPPoE dans la table de routage du CP. BGP recherche toujours dans la table de routage du CP le lancement de la session TCP. Par conséquent, BGP ne forme pas de session TCP.

  C'est pourquoi, BGP sur PPPoE n'est pas pris en charge.
- BGP n’est pas pris en charge sur les interfaces BVI ou de gestion uniquement.
- Pour éviter les oscillations de contiguïté dues aux mises à jour de routage abandonnées si la mise à jour de routage est supérieure à la MTU minimale sur le lien, configurez la même MTU sur les interfaces des deux côtés du lien.
- BGP avec PATH MTU (PMTU) peut entraîner des fluctuations de contiguïté en cas d’échec de la découverte de la MTU, en particulier avec le routage ECMP. Par conséquent, soyez prudent lorsque vous utilisez BGP, PMTU et ECMP, car des abandons de paquets peuvent se produire si la découverte de la MTU échoue pour une raison quelconque.
- La table BGP de l’unité membre n’est pas synchronisée avec la table de l’unité de contrôle. Seule sa table de routage est synchronisée avec celle de l’unité de contrôle.

Configurer le protocole BGP

Cette section décrit comment activer et configurer le processus BGP sur votre système.

Procédure

Étape 1 Activer BGP, à la page 1004.

Étape 2 Définir le meilleur chemin pour un processus de routage BGP, à la page 1005.

Étape 3 Configurer les listes de politiques, à la page 1006.

Étape 4 Configurer les filtres de chemin AS, à la page 1007.

Étape 5 Configurer les règles de communauté, à la page 1008.

Étape 6 Configurer les paramètres de la famille d'adresses IPv4, à la page 1009.

Étape 7 Configurer les paramètres de la famille d'adresses IPv6, à la page 1023.

Activer BGP

Cette section décrit les étapes requises pour activer le routage BGP, établir un processus de routage BGP et configurer les paramètres BGP généraux.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Les valeurs valides pour autonomous-num vont de 1 à 4294967295 et de 1.0 à XX.YY.

Étape 2 Ignorez les routes ayant des segments de chemin AS qui dépassent une valeur spécifiée :

bgp maxas-limit number

Exemple :

```
ciscoasa(config-router)# bgp maxas-limit 15
```

L'argument de nombre spécifie le nombre maximum de segments de système autonomes autorisés. Les valeurs valides sont comprises entre 1 et 254.

Étape 3 Journalisez les réinitialisations du voisin BGP :

changements journalisation voisin bgp

Étape 4 Activez BGP pour détecter automatiquement la meilleure MTU de chemin TCP pour chaque session BGP :

bgp transport path-mtu-discovery

Étape 5 Activez BGP pour mettre fin aux sessions BGP externes de tout homologue directement adjacent si le lien utilisé pour atteindre l'homologue tombe en panne; sans attendre l'expiration du délai d'attente :

bgp fast-external-fallover

Étape 6 Autorisez un processus de routage BGP à ignorer les mises à jour reçues d'un homologue BGP (eBGP) externe qui n'indique pas son numéro de système autonome (AS) comme premier segment de chemin AS dans l'attribut AS_PATH de la route entrante :

bgp enforce-first-as

Étape 7 Modifiez le format de correspondance d'affichage par défaut et d'expression régulière des numéros du système autonome BGP de 4 octets de texte (valeurs décimales) à la notation des points :

bgp asnotation dot

Étape 8 Ajustez les minuteries de réseau BGP :

timers bgp keepalive holdtime [min-holdtime]

Exemple :

```
ciscoasa(config-router)# timers bgp 80 120
```

- keepalive : la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive à son homologue. La valeur par défaut est de 60 secondes.
- holdtime : l'intervalle (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort. La valeur par défaut est de 180 secondes.
- (Facultatif) min-holdtime : l'intervalle minimal (en secondes) après l'absence de réception de message keepalive d'un voisin indiquant que l'ASA déclare un voisin mort.

  Remarque
  Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs.

Étape 9 Activez la capacité de redémarrage progressif de BGP :

bgp graceful-restart [restart-time seconds|stalepath-time seconds][all]

Exemple :

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- restart-time : période maximale (en secondes) pendant laquelle l'ASA attendra qu'un voisin compatible avec le redémarrage progressif reprenne son fonctionnement normal après un événement de redémarrage. La valeur par défaut est de 120 secondes. Les valeurs valides vont de 1 à 3 600 secondes.
- slatepath-time : période maximale (en secondes) pendant laquelle l'ASA conservera les chemins obsolètes pour un homologue en redémarrage. Tous les chemins obsolètes sont supprimés après l'expiration de cette minuterie. La valeur par défaut est 360 secondes. Les valeurs valides vont de 1 à 3 600 secondes.

Définir le meilleur chemin pour un processus de routage BGP

Cette section décrit les étapes requises pour configurer le meilleur chemin BGP. Pour en savoir plus sur le meilleur chemin, consultez Sélection du chemin BGP, à la page 1001.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Modifiez la valeur de préférence locale par défaut :

bgp default local-preference number

Exemple :

```
ciscoasa(config-router)# bgp default local-preference 500
```

L'argument number est toute valeur comprise entre 0 et 4294967295. Des valeurs plus élevées indiquent une préférence plus élevée.

La valeur par défaut est 100.

Étape 3 Activez la comparaison du Discriminateur multi-sortie (MED) entre les chemins appris des voisins dans différents systèmes autonomes :

bgp always-compare-med

Étape 4 Comparez les routes similaires reçues des homologues BGP externes (eBGP) pendant le processus de sélection du meilleur chemin et faites passer le meilleur chemin à la route ayant le plus petit ID de routeur :

bgp bestpath compare-routerid

Étape 5 Sélectionnez le meilleur chemin MED annoncé à partir de l'AS voisin :

bgp deterministic-med

Étape 6 Définissez un chemin avec un attribut MED manquant comme chemin le moins préféré :

bgp bestpath med missing-as-worst

Configurer les listes de politiques

Lorsqu'une liste de stratégie est référencée dans une carte de routage, toutes les déclarations de correspondance dans la liste de stratégie sont évaluées et traitées. Deux listes de politiques ou plus peuvent être configurées avec une carte de routage. Une liste de politiques peut également coexister avec d'autres instructions de mise en correspondance et d'ensemble préexistantes configurées dans la même carte de routage, mais en dehors de la liste de politiques. Cette section décrit les étapes requises pour configurer les listes de politiques.

Procédure

Étape 1 Créez une liste de politiques BGP.

policy-list *policy_list_name* {**permit** | **deny**}

Le mot clé **permit** autorise l'accès pour les conditions de correspondance.

Le mot clé **deny** refuse l'accès pour les conditions de correspondance.

Exemple :

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

Étape 2 Distribuez les routes dont le prochain saut se trouve hors de l'une des interfaces spécifiées :

match interface [*interface_name* [*interface_name*] […]]

Exemple :

```
ciscoasa(config-policy-list)# match interface outside
```

Étape 3 Redistribuez les routes en faisant correspondre l'un ou l'ensemble des éléments suivants : l'adresse de destination, l'adresse du routeur du saut suivant et la source du routeur/serveur d'accès :

match ip {**address** | **next-hop** | **route-source**}

Étape 4 Faites correspondre un chemin d'accès au système autonome BGP :

match as-path

Étape 5 Faites correspondre une communauté BGP :

match community {*community-list_name* | **exact-match**}

- *community-list_name* : une ou plusieurs listes de communautés.
- **exact-match** : indique qu'une correspondance exacte est requise. Toutes les communautés et seulement les communautés spécifiées doivent être présentes.

Exemple :

```
ciscoasa(config-policy-list)# match community ExampleCommunity1
```

Étape 6 Redistribuez les routes avec les mesures spécifiées :

match metric *metric* [*metric* […]]

Étape 7 Redistribuez les routes dans la table de routage qui correspondent aux balises spécifiées :

match tag *tag* [*tag* […]]

Configurer les filtres de chemin AS

Un filtre de chemin AS vous permet de filtrer le message de mise à jour de routage à l'aide de listes d'accès et d'examiner les préfixes individuels dans un message de mise à jour. Si un préfixe dans le message de mise à jour correspond aux critères de filtre, ce préfixe individuel est filtré ou accepté selon l'action configurée pour l'entrée de filtre. Cette section décrit les étapes requises pour configurer les filtres de chemin AS.

Remarque Les listes d'accès du chemin AS ne sont pas les mêmes que les ACL normales du pare-feu.

Procédure

Configurez un filtre de chemin de système autonome à l'aide d'une expression régulière dans le mode de configuration globale :

as-path access-list acl-number {permit|deny} regexp

Exemple :

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number* : numéro de liste d'accès du chemin AS. Cette valeur peut être comprise entre 1 et 500.
- regexp : expression régulière qui définit le filtre de chemin AS. Le numéro de système autonome est compris entre 1 et 65 535.

Configurer les règles de communauté

Une communauté étendue est un groupe plus vaste de destinations partageant un attribut commun. Vous pouvez utiliser les listes de communautés pour créer des groupes de communautés à utiliser dans une clause de correspondance d'une feuille de route. Tout comme une liste d'accès, une série de listes de communautés peut être créée. Les instructions sont vérifiées jusqu'à ce qu'une correspondance soit trouvée. Dès qu'une instruction est satisfaite, le test est terminé. Cette section décrit les étapes requises pour configurer les règles de communauté.

Procédure

Créez ou configurez une liste de communautés BGP et contrôlez l'accès à celle-ci :

community-list {standard| community list-name {deny|permit} [community-number] [AA:NN] [internet] [no-advertise][no-export]}| {expanded|expanded list-name {deny| permit}regexp}

Exemple :

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise no-export
```

- standard : configure une liste de communautés standard en utilisant un nombre allant de 1 à 99 pour identifier un ou plusieurs groupes de communautés autorisés ou refusés.

- (Facultatif) community-number : communauté sous forme de numéro de 32 bits allant de 1 à 4294967200. Une seule communauté peut être saisie ou plusieurs communautés peuvent être saisies, chacune séparée par un espace.
- AA:NN : un numéro de système autonome et un numéro de réseau saisis dans le nouveau format de communauté de 4 octets. Cette valeur est configurée avec deux nombres de 2 octets séparés par deux points. Un nombre de 1 à 65 535 peut être entré pour chaque numéro de 2 octets. Une seule communauté peut être saisie ou plusieurs communautés peuvent être saisies, chacune séparée par un espace.
- (Facultatif) internet : spécifie la communauté Internet. Les routages de cette communauté sont annoncés à tous les homologues (internes et externes).
- (Facultatif) no-advertise : spécifie la communauté sans publicité. Les routages de cette communauté ne sont annoncés à aucun homologue (interne ou externe).
- (Facultatif) no-export : spécifie la communauté sans exportation. Les routes avec cette communauté sont annoncées uniquement aux homologues dans le même système autonome ou uniquement aux autres systèmes sous-autonomes d'une confédération. Ces routes ne sont pas annoncées aux homologues externes.
- (Facultatif) expanded : configure un numéro de liste de communautés étendu de 100 à 500 pour identifier un ou plusieurs groupes de communautés autorisés ou refusés.
- regexp : expression régulière qui définit le filtre de chemin AS. Le numéro de système autonome est compris entre 1 et 65 535.

Remarque
Les expressions régulières ne peuvent être utilisées qu'avec les listes de communautés étendues.

Configurer les paramètres de la famille d'adresses IPv4

Les paramètres IPv4 pour le BGP peuvent être configurés à partir de l'option de famille IPv4 dans la configuration du BGP. La section de la famille IPv4 comprend des sous-sections pour les paramètres généraux, les paramètres d'adresse d'agrégation, les paramètres de filtrage et les paramètres de voisin. Chacune de ces sous-sections vous permet de personnaliser les paramètres propres à la famille IPv4.

Configurer les paramètres généraux de la famille IPv4

Cette section décrit les étapes requises pour configurer les paramètres IPv4 généraux.

Procédure

Étape 1 Activez un processus de routage BGP, qui place le routeur en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 (Facultatif) Configurez un ID de routeur fixe pour le processus de routage BGP local :

bgp router-id A.B.C.D

Exemple :

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

L'argument A.B.C.D spécifie un identifiant de routeur sous la forme d'une adresse IP. Si vous ne spécifiez pas d'ID de routeur, il est automatiquement attribué.

Étape 4 (Facultatif) Configurez un ensemble d'adresses IP en grappe en mode d'interface individuelle (L3) :

bgp router-id cluster-pool

Exemple :

```
ciscoasa(config-router-af)# bgp router-id cp
```

Remarque
Dans une grappe L3, vous ne pouvez pas définir un voisin BGP comme l'une des adresses IP de l'ensemble de grappe.

Étape 5 Configurez la distance administrative des routes BGP :

distance bgp external-distance internal-distance local-distance

Exemple :

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance : distance administrative pour les routes BGP externes. Les routes sont externes lorsqu'elles sont apprises à partir d'un système autonome externe. La plage de valeurs pour cet arguments est comprise entre 1 et 255.
- internal-distance : distance administrative pour les routes BGP internes. Les routes sont internes lorsqu'elles sont apprises de l'homologue dans le système autonome local. La plage de valeurs pour cet arguments est comprise entre 1 et 255.
- local-distance : distance administrative pour les routes BGP locales. Les routes locales sont les réseaux répertoriés avec une commande de configuration de routeur de réseau, souvent comme portes dérobées, pour le routeur ou pour les réseaux qui sont redistribués à partir d'un autre processus. La plage de valeurs pour cet arguments est comprise entre 1 et 255.

Étape 6 Modifiez les valeurs des mesures et des balises lorsque le tableau de routage IP est mis à jour avec les routes apprises du protocole BGP :

table-map {WORD|route-map_name}

Exemple :

```
ciscoasa(config-router-af)# table-map example1
```

L'argument route-map_name spécifie le nom de la carte de routage de la commande route-map.

Étape 7 Configurez un processus de routage BGP pour distribuer une route par défaut (réseau 0.0.0.0) :

default-information originate

Étape 8 Configurez la synthèse automatique des routes de sous-réseau dans les routes au niveau du réseau :

auto-summary

Étape 9 Supprimez l'annonce des routes qui ne sont pas installées dans la base d'informations de routage (RIB) :

bgp suppress-inactive

Étape 10 Synchronisez le BGP avec votre système IGP (protocole de passerelle intérieure) :

synchronisation

Étape 11 Configurez la redistribution iBGP dans un IGP, tel que OSPF :

bgp redistribute-internal

Étape 12 Configurez des intervalles d'analyse des routeurs BGP pour la validation du saut suivant :

bgp scan-time scanner-interval

Exemple :

```
ciscoasa(config-router-af)# bgp scan-time 15
```

L'argument scanner-interval spécifie l'intervalle d'analyse des renseignements de routage BGP. Les valeurs valides sont comprises entre 5 et 60 secondes. La valeur par défaut est de 60 secondes.

Étape 13 Configurez le suivi des adresses du saut suivant du protocole BGP :

bgp nexthop trigger {delay seconds|enable}

Exemple :

```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- trigger : spécifie l'utilisation du suivi d'adresses du saut suivant du protocole BGP. Utilisez ce mot clé avec le mot clé delay pour modifier le délai de suivi du saut suivant. Utilisez ce mot clé avec le mot clé enable pour activer le suivi d'adresses du saut suivant.
- delay : modifie l'intervalle de délai entre les vérifications sur les routes de saut suivant mises à jour installées dans la table de routage.
- seconds : spécifie le délai en secondes. La plage se situe entre 0 et 100. La valeur par défaut est 5.
- enable : active immédiatement le suivi des adresses du saut suivant du protocole BGP.

Étape 14 Contrôlez le nombre maximum de routes iBGP parallèles qui peuvent être installées dans une table de routage :

maximum-paths {number_of_paths|ibgp number_of_paths}

Exemple :

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

Remarque
Si le mot clé ibgp n'est pas utilisé, l'argument number_of_paths contrôle le nombre maximum de routes EBGP parallèles.

L'argument number_of_paths spécifie le nombre de routes à installer dans la table de routage. Les valeurs valides sont comprises entre 1 et 8.

Configurer les paramètres d'adresse globale de la famille IPv4

Cette section décrit les étapes requises pour définir l'agrégation de routes spécifiques en une seule route.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Créez une entrée agrégée dans une base de données BGP :

aggregate-address address mask [as-set][summary-only][suppress-map map-name][advertise-map map-name][attribute-map map-name]

Exemple :

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only
 suppress-map example1 advertise-map example1 attribute-map example1
```

- address : l'adresse agrégée.
- mask : le masque agrégé.
- map-name : la carte de routage.
- (Facultatif) as-set : génère des renseignements sur le chemin de définition du système autonome.

- (Facultatif) summary-only : filtre toutes les routes plus spécifiques à partir des mises à jour.
- (Facultatif) Suppress-map map-name : spécifie le nom de la carte de routage utilisée pour sélectionner les routes à supprimer.
- (Facultatif) Advertise-map map-name : spécifie le nom de la carte de routage utilisée pour sélectionner les routes afin de créer les communautés d'origine AS_SET.
- (Facultatif) Attribute-map map-name : spécifie le nom de la carte de routage utilisée pour définir l'attribut de la route agrégée.

Configurer les paramètres de filtrage de la famille IPv4

Cette section décrit les étapes requises pour filtrer les routes ou les réseaux reçus dans les mises à jour BGP entrantes.

Procédure

Étape 1 Activez un processus de routage BGP et passez en mode de configuration du routeur :

router bgp *autonomous-num*

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [**unicast**]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Filtrez les routes ou les réseaux reçus dans les mises à jour BGP entrantes ou annoncés dans les mises à jour BGP sortantes :

distribute-list *acl-number* {**in** | **out**} [*protocol process-number* | **connected** | **static**]

L'argument *acl-number* spécifie le numéro de la liste d'accès IP. La liste d'accès définit les réseaux à recevoir et ceux à supprimer dans les mises à jour de routage.

Le mot clé **in** spécifie que le filtre doit être appliqué aux mises à jour BGP entrantes et **out** spécifie que le filtre doit être appliqué aux mises à jour BGP sortantes.

Pour les filtres sortants, vous pouvez éventuellement spécifier un protocole (**bgp**, **eigrp**, **ospf** ou **rip**) avec un numéro de processus (à l'exception du protocole RIP) à appliquer à la liste de distribution. Vous pouvez également filtrer selon que les homologues et les réseaux ont été appris par les routes **connected** ou **static**.

Exemple :

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

Configurer les paramètres de voisin BGP de la famille IPv4

Cette section décrit les étapes requises pour définir les voisins BGP et les paramètres de voisins.

Procédure

Étape 1 Activez un processus de routage BGP, qui place le routeur en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Ajoutez une entrée au tableau de voisins BGP :

neighbor ip-address remote-as autonomous-number

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

Étape 4 (Facultatif) Désactivez un groupe de voisins ou d'homologues :

neighbor ip-address shutdown

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

Étape 5 Échangez des renseignements avec un voisin BGP :

neighbor ip-address activate

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

Étape 6 Activez ou désactivez la fonctionnalité de redémarrage progressif du protocole de passerelle frontière (BGP) pour un voisin BGP :

neighbor ip-address ha-mode graceful-restart [disable]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

(Facultatif) Le mot clé disable désactive la fonctionnalité de redémarrage progressif du BGP pour un voisin.

Étape 7 Distribuez les renseignements sur le voisin BGP comme spécifiés dans une liste d'accès :

neighbor {ip-address} distribute-list {access-list-name}{in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in
```

- access-list-number : le numéro d'une liste d'accès standard ou étendue. La plage d'un numéro de liste d'accès standard va de 1 à 99. La plage d'un numéro de liste d'accès étendue va de 100 à 199.
- expanded-list-number : le numéro d'une liste d'accès étendue. La plage d'une liste d'accès étendue va de 1 300 à 2 699.
- access-list-name : le nom d'une liste d'accès standard ou étendue.
- prefix-list-name : le nom d'une liste de préfixes BGP.
- in : la liste d'accès est appliquée aux annonces entrantes de ce voisin.
- out : signifie que la liste d'accès est appliquée aux annonces sortantes vers ce voisin.

Étape 8 Appliquez une carte de routage aux routes entrantes ou sortantes :

neighbor {ip-address} route-map map-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

Le mot clé dans applique une carte de routage aux routes entrantes.

Le mot clé out applique une carte de routage aux routes sortantes.

Étape 9 Distribuez les renseignements sur le voisin BGP comme spécifiés dans une liste de préfixes :

neighbor {ip-address} prefix-list prefix-list-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

Le mot clé in implique que la liste de préfixes soit appliquée aux annonces entrantes de ce voisin.

Le mot clé out implique que la liste de préfixes soit appliquée aux annonces sortantes de ce voisin.

Étape 10 Configurez une liste de filtres :

neighbor {ip-address} filter-list access-list-number {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in
```

- access-list-name : spécifie le numéro d'une liste d'accès de chemin au système autonome. Vous définissez cette liste d'accès avec la commande ip as-path access-list.
- in : signifie que la liste d'accès est appliquée aux annonces entrantes de ce voisin.
- out : signifie que la liste d'accès est appliquée aux annonces sortantes vers ce voisin.

Étape 11 Contrôlez le nombre de préfixes pouvant être reçus d'un voisin.

neighbor {ip-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- maximum : le nombre maximum de préfixes autorisés pour ce voisin.
- (Facultatif) threshold : entier indiquant à quel pourcentage du maximum le routeur commence à générer un message d'avertissement. La plage se situe entre 1 et 100; la valeur par défaut est de 75 (pour cent).
- (Facultatif) restart interval : valeur entière (en minutes) qui spécifie l'intervalle de temps après lequel le voisin BGP redémarre.
- (Facultatif) warning-only : permet au routeur de générer un message de journal lorsque le nombre maximum de préfixes est dépassé, au lieu de mettre fin à l'homologation.

Étape 12 Autorisez un haut-parleur BGP (le routeur local) à envoyer la route par défaut 0.0.0.0 à un voisin pour qu'il l'utilise comme route par défaut :

neighbor {ip-address} default-originate [route-map map-name]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

L'argument map-name est le nom de la carte de routage. La carte de routage permet l'injection conditionnelle de la route 0.0.0.0.

Étape 13 Définissez l'intervalle minimum entre l'envoi des mises à jour de routage BGP :

neighbor {ip-address} advertisement-interval seconds

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

L'argument seconds est le temps (en secondes). Les valeurs valides sont comprises entre 0 et 600.

Étape 14 Annoncez les routes dans le tableau BGP qui correspondent à la carte de routes configurée :

neighbor {ip-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name : le nom de la carte de routage qui sera annoncée si les conditions de la carte existante ou inexistante sont remplies.
- exist-map map name : le nom de la carte existante qui est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- non-exist-map map name : le nom de la carte inexistante qui est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- (Facultatif) check all paths : active la vérification de tous les chemins par la carte existante avec un préfixe dans le tableau BGP.

Étape 15 Supprimez les numéros de système autonome privés des mises à jour de routage sortant :

neighbor {ip-address} remove-private-as

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

Étape 16 Définissez les minuteries pour un homologue ou un groupe d'homologues BGP spécifique.

neighbor {ip-address} timers keepalive holdtime min holdtime

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- keepalive : la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive à son homologue. La valeur par défaut est de 60 secondes. Les valeurs valides sont comprises entre 0 et 65 535.
- holdtime : l'intervalle (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort. La valeur par défaut est de 180 secondes.
- min holdtime : l'intervalle minimum (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort.

  Remarque
  Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs.

Étape 17 Activez l'authentification Message Digest 5 (MD5) sur une connexion TCP entre deux homologues BGP :

neighbor {ip-address} password string

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

La chaîne d'argument est un mot de passe sensible à la casse pouvant comporter jusqu'à 25 caractères lorsque la commande de service password-encryption est activée et jusqu'à 81 caractères lorsqu'elle ne l'est pas. La chaîne peut contenir n'importe quel caractère alphanumérique, y compris des espaces.

Remarque
Lorsque vous définissez le premier caractère du mot de passe comme un nombre, ne fournissez pas d'espace immédiatement après le nombre. En d'autres termes, vous ne pouvez pas spécifier de mot de passe au format number-space-anything. L'espace après le numéro peut faire échouer l'authentification.

Étape 18 Précisez que les attributs de communautés doivent être envoyés à un voisin BGP :

neighbor {ip-address} send-community

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

Étape 19 Configurez le routeur comme prochain saut pour un voisin ou un groupe d'homologues utilisant BGP :

neighbor {ip-address}next-hop-self

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

Étape 20 Acceptez et tentez des connexions BGP avec des homologues externes résidant sur des réseaux qui ne sont pas connectés directement :

neighbor {ip-address} ebgp-multihop [ttl]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

L'argument ttl spécifie la durée de vie dans une plage comprise entre 1 et 255 sauts.

Étape 21 Désactivez la vérification de connexion pour établir une session d'homologation eBGP avec un homologue à saut unique qui utilise une interface de boucle avec retour :

neighbor {ip-address} disable-connected-check

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

Étape 22 Sécurisez une session d'homologation BGP et configurez le nombre maximum de sauts qui séparent deux homologues BGP (eBGP) externes :

neighbor {ip-address} ttl-security hops hop-count

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

L'argument hop-count est le nombre de sauts qui séparent les homologues eBGP. La valeur de la TTL est calculée par le routeur à partir de l'argument hop-count configuré. Les valeurs valides sont comprises entre 1 et 254.

Étape 23 Attribuez une pondération à une connexion de voisin :

neighbor {ip-address} weight number

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

Le numéro d'argument est la pondération à attribuer à une connexion de voisin. Les valeurs valides sont comprises entre 0 et 65 535.

Étape 24 Configurez l'ASA pour accepter uniquement une version BGP particulière :

neighbor {ip-address} version number

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

Le numéro d'argument spécifie le numéro de version du BGP. La version peut être définie sur 2 pour forcer le logiciel à utiliser uniquement la version 2 avec le voisin spécifié. La valeur par défaut est d'utiliser la version 4 et de négocier dynamiquement à la baisse jusqu'à la version 2 si nécessaire.

Étape 25 Activez une option de session de transport TCP pour une session BGP :

neighbor {ip-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- connection-mode : le type de connexion (active ou passive).
- path-mtu-discovery : active la découverte de l'unité de transfert maximale (MTU) du chemin de transport TCP. La découverte MTU du chemin TCP est activée par défaut.
- (Facultatif) disable : désactive la découverte MTU du chemin TCP.

Étape 26 Personnalisez l'attribut AS_PATH pour les routes reçues d'un voisin externe du protocole de passerelle frontière (eBGP) :

neighbor {ip-address} local-as [autonomous-system-number[no-prepend]]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- (Facultatif) autonomous-system-number : le numéro d'un système autonome à ajouter au début de l'attribut AS_PATH. La plage de valeurs pour cet argument est tout numéro de système autonome valide compris entre 1 et 4294967295 ou 1.0 à XX.YY.
- (Facultatif) no-prepend : n'ajoute pas le numéro de système autonome local à aucune route reçue du voisin eBGP.

Étape 27 Pour mettre à jour une interface en tant que source pour un voisinage BGP :

neighbor *ip_address* **update-source** *interface_name*

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 update-source loop1
```

L'argument *interface_name* est le nom de l'interface que le voisin BGP utilise comme source pour le routage BGP.

Remarque
Si vous mettez à jour l'interface de boucle avec retour comme source pour le voisinage BGP, l'adresse IP de l'interface de boucle avec retour est annoncée sur le réseau. L'interface de boucle avec retour agit en tant qu'homologue eBGP et participe au routage. Comme l'interface de boucle avec retour est stable lorsqu'elle est activée et reste disponible jusqu'à ce qu'elle soit administrativement arrêtée, l'ASA est toujours accessible sur l'adresse IP de l'interface de boucle avec retour.

Configurer les paramètres réseau IPv4

Cette section décrit les étapes requises pour définir les réseaux à annoncer par le processus de routage de BGP.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Précisez les réseaux à annoncer par les processus de routage de BGP :

network {network-number [mask network-mask]}[route-map map-tag]

Exemple :

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

Remarque
Pour qu'un préfixe de réseau soit annoncé, une voie de routage vers le périphérique doit exister dans la table de routage.

- network-number : le réseau que BGP annoncera.
- (Facultatif) network-mask : le masque de réseau ou de sous-réseau avec l'adresse de masque.

- (Facultatif) map-tag : l'identifiant d'une carte de routage configurée. Il faut examiner la carte de routage pour filtrer les réseaux à annoncer. S'ils ne sont pas spécifiés, tous les réseaux sont annoncés.

Configurer les paramètres de redistribution IPv4

Cette section décrit les étapes nécessaires pour définir les conditions de redistribution des routes d'un autre domaine de routage vers BGP.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Redistribuez les routes d'un autre domaine de routage dans un système autonome BGP :

redistribute protocol [process-id] [metric] [route-map [map-tag]]

Exemple :

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol : le protocole source à partir duquel les routes sont redistribuées. Il peut s'agir de l'une des options suivantes : Connected (connecté), EIGRP, OSPF, RIP ou Static (statique).
- (Facultatif) process-id : un nom pour le processus de routage spécifique.
- (Facultatif) metric : la mesure pour la route redistribuée.
- (Facultatif) map-tag : l'identifiant d'une carte de routage configurée.

Remarque

Il faut examiner la carte de routage pour filtrer les réseaux à redistribuer. S'ils ne sont pas spécifiés, tous les réseaux sont redistribués.

Configurer les paramètres d'injection de route IPv4

Cette section décrit les étapes nécessaires pour définir les routes à injecter de manière conditionnelle dans la table de routage de BGP.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP version 4 (IPv4) standard :

address-family ipv4 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

Le mot clé unicast spécifie les préfixes d'adresse de monodiffusion IPv4. Il s'agit de la valeur par défaut, même si elle n'est pas spécifiée.

Étape 3 Configurez l'injection conditionnelle de routes pour injecter des routes plus précises dans une table de routage de BGP :

bgp inject-map inject-map exist-map exist-map [copy-attributes]

Exemple :

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map : le nom de la carte de routage qui spécifie les préfixes à injecter dans la table de routage de BGP locale.
- exist-map : le nom de la carte de routage contenant les préfixes que le locuteur BGP suivra.
- (Facultatif) copy-attributes : configure la route injectée pour hériter des attributs de la route agrégée.

Configurer les paramètres de la famille d'adresses IPv6

Les paramètres IPv6 pour le BGP peuvent être configurés à partir de l'option de famille IPv6 dans la configuration du BGP. La section de la famille IPv6 comprend des sous-sections pour les paramètres généraux, les paramètres d'adresse d'agrégation et les paramètres de voisin. Chacune de ces sous-sections vous permet de personnaliser les paramètres propres à la famille IPv6.

Cette section décrit comment personnaliser les paramètres de famille IPv6 du BGP.

Configurer les paramètres généraux de la famille IPv6

Cette section décrit les étapes requises pour configurer les paramètres IPv6 généraux.

Procédure

Étape 1 Activez un processus de routage BGP, qui place le routeur en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Étape 3 Configurez la distance administrative des routes BGP :

distance bgp external-distance internal-distance local-distance

Exemple :

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance : distance administrative pour les routes BGP externes. Les routes sont externes lorsqu'elles sont apprises à partir d'un système autonome externe. La plage de valeurs pour cet arguments est comprise entre 1 et 255.
- internal-distance : distance administrative pour les routes BGP internes. Les routes sont internes lorsqu'elles sont apprises de l'homologue dans le système autonome local. La plage de valeurs pour cet arguments est comprise entre 1 et 255.
- local-distance : distance administrative pour les routes BGP locales. Les routes locales sont les réseaux répertoriés avec une commande de configuration de routeur de réseau, souvent comme portes dérobées, pour le routeur ou pour les réseaux qui sont redistribués à partir d'un autre processus. La plage de valeurs pour cet arguments est comprise entre 1 et 255.

Étape 4 (Facultatif) Configurez un processus de routage BGP pour distribuer une route par défaut (réseau 0.0.0.0) :

default-information originate

Étape 5 (Facultatif) Supprimez l'annonce des routes qui ne sont pas installées dans la base d'informations de routage (RIB) :

bgp suppress-inactive

Étape 6 Synchronisez le BGP avec votre système IGP (protocole de passerelle intérieure) :

synchronisation

Étape 7 Configurez la redistribution iBGP dans un IGP, tel que OSPF :

bgp redistribute-internal

Étape 8 Configurez des intervalles d'analyse des routeurs BGP pour la validation du saut suivant :

bgp scan-time scanner-interval

Exemple :

```
ciscoasa(config-router-af)# bgp scan-time 15
```

Valeurs valides pour l'argument d'intervalle d'analyse de 5 à 60 secondes. La valeur par défaut est de 60 secondes.

Étape 9 Contrôlez le nombre maximum de routes iBGP parallèles qui peuvent être installées dans une table de routage :

maximum-paths {number_of_paths|ibgp number_of_paths}

Exemple :

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

Les valeurs valides pour l'argument number_of_paths sont comprises entre 1 et 8.

Si le mot clé ibgp n'est pas utilisé, l'argument number_of_paths contrôle le nombre maximum de routes EBGP parallèles.

Configurer les paramètres d'adresse globale de la famille IPv6

Cette section décrit les étapes requises pour définir l'agrégation de routes spécifiques en une seule route.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 unicast

Étape 3 Créez une entrée agrégée dans une base de données BGP :

aggregate-address ipv6-address/cidr [as-set][summary-only][suppress-map map-name][advertise-map ipv6-map-name][attribute-map map-name]

Exemple :

```
ciscoasa(config-router-af) aggregate-address 2000::1/8 summary-only
```

- address : l'adresse IPv6 agrégée.
- (Facultatif) as-set : génère des renseignements sur le chemin de définition du système autonome.
- (Facultatif) summary-only : filtre toutes les routes plus spécifiques à partir des mises à jour.
- (Facultatif) suppress-map map-name : spécifie le nom de la carte de routage utilisée pour sélectionner les routes à supprimer.
- (Facultatif) advertise-map map-name : spécifie le nom de la carte de routage utilisée pour sélectionner les routes afin de créer les communautés d'origine AS_SET.
- (Facultatif) attribute-map map-name : spécifie le nom de la carte de routage utilisée pour définir l'attribut de la route agrégée.

Étape 4 Définissez l'intervalle auquel les routes BGP seront agrégées :

bgp aggregate-timer seconds

Exemple :

```
ciscoasa(config-router-af)bgp aggregate-timer 20
```

Configurer les paramètres de voisin BGP de la famille IPv6

Cette section décrit les étapes requises pour définir les voisins BGP et les paramètres de voisins.

Procédure

Étape 1 Activez un processus de routage BGP, qui place le routeur en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Étape 3 Ajoutez une entrée au tableau de voisins BGP :

neighbor ipv6-address remote-as autonomous-number

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1/8 remote-as 3
```

L'argument ipv6-address spécifie l'adresse IPv6 du prochain saut qui peut être utilisé pour atteindre le réseau spécifié. L'adresse IPv6 du prochain saut ne doit pas être connectée directement; une récursivité est effectuée pour trouver l'adresse IPv6 du saut suivant directement connecté. Lorsqu'un type d'interface et un numéro d'interface sont spécifiés, vous pouvez éventuellement spécifier l'adresse IPv6 du prochain saut vers lequel les paquets sont sortants. Vous devez préciser un type d'interface et un numéro d'interface lors de l'utilisation d'une adresse Link-Local comme prochain saut (le prochain saut de Link-Local doit également être un appareil adjacent).

Remarque
Cet argument doit être dans la forme documentée dans la RFC 2373, où l'adresse est spécifiée en hexadécimal en utilisant des valeurs de 16 bits entre les deux-points.

Étape 4 (Facultatif) Désactivez un groupe de voisins ou d'homologues :

neighbor ipv6-address shutdown

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1/8 shutdown 3
```

Étape 5 Échangez des renseignements avec un voisin BGP :

neighbor ipv6-address activate

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1/8 activate
```

Étape 6 Activez ou désactivez la fonctionnalité de redémarrage progressif du protocole de passerelle frontière (BGP) pour un voisin BGP :

neighbor {ip-address} ha-mode graceful-restart [disable]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1/8 ha-mode graceful-restart
```

(Facultatif) Le mot clé disable désactive la fonctionnalité de redémarrage progressif du BGP pour un voisin.

Étape 7 Appliquez une carte de routage aux routes entrantes ou sortantes :

neighbor {ipv6-address} route-map map-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 route-map example1 in
```

Le mot clé dans applique une carte de routage aux routes entrantes.

Le mot clé out applique une carte de routage aux routes sortantes.

Étape 8 Distribuez les renseignements sur le voisin BGP comme spécifiés dans une liste de préfixes :

neighbor {ipv6-address} prefix-list prefix-list-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 prefix-list NewPrefixList in
```

Le mot clé in implique que la liste de préfixes soit appliquée aux annonces entrantes de ce voisin.

Le mot clé out implique que la liste de préfixes soit appliquée aux annonces sortantes de ce voisin.

Étape 9 Configurez une liste de filtres :

neighbor {ipv6-address} filter-list access-list-name {in|out}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 filter-list 5 in
```

- access-list-name : spécifie le numéro d'une liste d'accès de chemin au système autonome. Vous définissez cette liste d'accès avec la commande ip as-path access-list.
- in : signifie que la liste d'accès est appliquée aux annonces entrantes de ce voisin.
- out : signifie que la liste d'accès est appliquée aux annonces sortantes vers ce voisin.

Étape 10 Contrôlez le nombre de préfixes pouvant être reçus d'un voisin.

neighbor {ipv6-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 maximum-prefix 7 75 restart 12
```

- maximum : le nombre maximum de préfixes autorisés pour ce voisin.
- (Facultatif) threshold : entier indiquant à quel pourcentage du maximum le routeur commence à générer un message d'avertissement. La plage se situe entre 1 et 100; la valeur par défaut est de 75 (pour cent).
- (Facultatif) restart interval : valeur entière (en minutes) qui spécifie l'intervalle de temps après lequel le voisin BGP redémarre.
- (Facultatif) warning-only : permet au routeur de générer un message de journal lorsque le nombre maximum de préfixes est dépassé, au lieu de mettre fin à l'homologation.

Étape 11 Autorisez un haut-parleur BGP (le routeur local) à envoyer la route par défaut 0.0.0.0 à un voisin pour qu'il l'utilise comme route par défaut :

neighbor {ipv6-address} default-originate [route-map map-name]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 default-originate route-map example1
```

L'argument map-name est le nom de la carte de routage. La carte de routage permet l'injection conditionnelle de la route 0.0.0.0.

Étape 12 Définissez l'intervalle minimum entre l'envoi des mises à jour de routage BGP :

neighbor {ipv6-address} advertisement-interval seconds

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 advertisement-interval 15
```

L'argument seconds est le temps (en secondes). Les valeurs valides sont comprises entre 0 et 600.

Étape 13 Supprimez les numéros de système autonome privés des mises à jour de routage sortant :

neighbor {ipv6-address} remove-private-as

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 remove-private-as
```

Étape 14 Annoncez les routes dans le tableau BGP qui correspondent à la carte de routes configurée :

neighbor {ipv6-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name : le nom de la carte de routage qui sera annoncée si les conditions de la carte existante ou inexistante sont remplies.
- exist-map map name : le nom de la carte existante qui est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- non-exist-map map name : le nom de la carte inexistante qui est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée ou non.
- (Facultatif) check all paths : active la vérification de tous les chemins par la carte existante avec un préfixe dans le tableau BGP.

Étape 15 Définissez les minuteries pour un homologue ou un groupe d'homologues BGP spécifique.

neighbor {ipv6-address} timers keepalive holdtime min holdtime

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 timers 15 20 12
```

- keepalive : la fréquence (en secondes) à laquelle l'ASA envoie des messages keepalive à son homologue. La valeur par défaut est de 60 secondes. Les valeurs valides sont comprises entre 0 et 65 535.

- holdtime : l'intervalle (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort. La valeur par défaut est de 180 secondes.
- min holdtime : l'intervalle minimum (en secondes) après l'absence de réception de message keepalive indiquant que l'ASA déclare un homologue comme mort.

Remarque
Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs.

Étape 16 Activez l'authentification Message Digest 5 (MD5) sur une connexion TCP entre deux homologues BGP :

neighbor {ipv6-address} password string

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 password test
```

La chaîne d'argument est un mot de passe sensible à la casse pouvant comporter jusqu'à 25 caractères lorsque la commande de service password-encryption est activée et jusqu'à 81 caractères lorsqu'elle ne l'est pas. La chaîne peut contenir n'importe quel caractère alphanumérique, y compris des espaces.

Remarque
Lorsque vous définissez le premier caractère du mot de passe comme un nombre, ne fournissez pas d'espace immédiatement après le nombre. En d'autres termes, vous ne pouvez pas spécifier de mot de passe au format number-space-anything. L'espace après le numéro peut faire échouer l'authentification.

Étape 17 Précisez que les attributs de communautés doivent être envoyés à un voisin BGP :

neighbor {ipv6-address} send-community [standard]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 send-community
```

(Facultatif) mot clé standard : seules les communautés standard seront envoyées.

Étape 18 Configurez le routeur comme prochain saut pour un voisin ou un groupe d'homologues utilisant BGP :

neighbor {ipv6-address}next-hop-self

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 next-hop-self
```

Étape 19 Acceptez et tentez des connexions BGP avec des homologues externes résidant sur des réseaux qui ne sont pas connectés directement :

neighbor {ipv6-address} ebgp-multihop [ttl]

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 ebgp-multihop 5
```

L'argument ttl spécifie la durée de vie dans une plage comprise entre 1 et 255 sauts.

Étape 20 Désactivez la vérification de connexion pour établir une session d'homologation eBGP avec un homologue à saut unique qui utilise une interface de boucle avec retour :

neighbor {ipv6-address} disable-connected-check

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 disable-connected-check
```

Étape 21 Sécurisez une session d'homologation BGP et configurez le nombre maximum de sauts qui séparent deux homologues BGP (eBGP) externes :

neighbor {ipv6-address} ttl-security hops hop-count

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

L'argument hop-count est le nombre de sauts qui séparent les homologues eBGP. La valeur de la TTL est calculée par le routeur à partir de l'argument hop-count configuré. Les valeurs valides sont comprises entre 1 et 254.

Étape 22 Attribuez une pondération à une connexion de voisin :

neighbor {ipv6-address} weight number

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 weight 30
```

Le numéro d'argument est la pondération à attribuer à une connexion de voisin. Les valeurs valides sont comprises entre 0 et 65 535.

Étape 23 Configurez l'ASA pour accepter uniquement une version BGP particulière :

neighbor {ipv6-address} version number

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 version 4
```

Le numéro d'argument spécifie le numéro de version du BGP. La valeur par défaut est la version 4. Actuellement, seule la version 4 de BGP est prise en charge.

Étape 24 Activez une option de session de transport TCP pour une session BGP :

neighbor {ipv6-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 transport connection-mode active
```

- connection-mode : le type de connexion (active ou passive).
- path-mtu-discovery : active la découverte de l'unité de transfert maximale (MTU) du chemin de transport TCP. La découverte MTU du chemin TCP est activée par défaut.

- (Facultatif) disable : désactive la découverte MTU du chemin TCP.

Étape 25 Personnalisez l'attribut AS_PATH pour les routes reçues d'un voisin externe du protocole de passerelle frontière (eBGP) :

neighbor {ipv6-address} local-as [autonomous-system-number[no-prepend]]

Exemple :

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- (Facultatif) autonomous-system-number : le numéro d'un système autonome à ajouter au début de l'attribut AS_PATH. La plage de valeurs pour cet argument est tout numéro de système autonome valide compris entre 1 et 4294967295 ou 1.0 à XX.YY.
- (Facultatif) no-prepend : n'ajoute pas le numéro de système autonome local à aucune route reçue du voisin eBGP.

Mise en garde
BGP ajoute au début le numéro de système autonome de chaque réseau BGP qu'une route traverse pour conserver les renseignements sur l'accessibilité du réseau et pour éviter les boucles de routage. Cette commande ne doit être configurée que pour la migration du système autonome et doit être supprimée une fois la transition terminée. Cette procédure ne doit être tentée que par un opérateur de réseau expérimenté. Des boucles de routage peuvent être créées par une configuration inadéquate.

Étape 26 Pour mettre à jour une interface en tant que source pour le voisinage BGP :

neighbor {ipv6-address} update-source {interface name}

Exemple :

```
ciscoasa(config-router-af)# neighbor 2000::1 update-source loop1
```

L'argument interface name spécifie le nom de l'interface que le voisin BGP utilise comme source pour le routage BGP.

Remarque
Si vous mettez à jour l'interface de boucle avec retour comme source pour le voisinage BGP, l'adresse IP de l'interface de boucle avec retour est annoncée sur le réseau. L'interface de boucle avec retour agit en tant qu'homologue eBGP et participe au routage. Comme l'interface de boucle avec retour est stable lorsqu'elle est activée et reste disponible jusqu'à ce qu'elle soit administrativement arrêtée, l'ASA est toujours accessible sur l'adresse IP de l'interface de boucle avec retour.

Configurer les paramètres réseau IPv6

Cette section décrit les étapes requises pour définir les réseaux à annoncer par le processus de routage de BGP.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp *autonomous-num*

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Étape 3 Précisez les réseaux à annoncer par les processus de routage de BGP :

network {*prefix_delegation_name* [*subnet_prefix*/*prefix_length*] | *ipv6_prefix*/*prefix_length*} [**route-map** *route_map_name*]

Exemple :

```
ciscoasa(config-router-af)# network 2001:1/64 route-map test_route_map
ciscoasa(config-router-af)# network outside-prefix 1::/64
ciscoasa(config-router-af)# network outside-prefix 2::/64
```

- *prefix_delegation_name* : si vous activez le client de délégation de préfixe DHCPv6 (**ipv6 dhcp client pd**), vous pouvez annoncer le ou les préfixes. Pour faire figurer dans un sous-réseau le préfixe, spécifiez *subnet_prefix*/*prefix_length*.
- *ipv6 network*/*prefix_length* : le réseau que BGP annoncera.
- (Facultatif) **route-map** *name* : l'identifiant d'une carte de routage configurée. Il faut examiner la carte de routage pour filtrer les réseaux à annoncer. S'ils ne sont pas spécifiés, tous les réseaux sont annoncés.

Configurer les paramètres de redistribution IPv6

Cette section décrit les étapes nécessaires pour définir les conditions de redistribution des routes d'un autre domaine de routage vers BGP.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv6[unicast]
```

Étape 3 Redistribuez les routes d'un autre domaine de routage dans un système autonome BGP :

```
redistribute protocol [process-id][autonomous-num][metric metric value][match{internal|
external1|external2|NSSA external 1|NSSA external 2}][route-map [map-tag]][subnets]
```

Exemple :

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol : le protocole source à partir duquel les routes sont redistribuées. Il peut s'agir de l'une des options suivantes : Connected (connecté), EIGRP, OSPF, RIP ou Static (statique).
- (Facultatif) process-id : pour le protocole ospf, il s'agit d'un ID de processus OSPF approprié à partir duquel les routes doivent être redistribuées. Cela identifie le processus de routage. Cette valeur prend la forme d'un nombre décimal différent de zéro.

  Remarque
  Cette valeur est renseignée automatiquement pour les autres protocoles.

- (Facultatif) metric metric value : lors de la redistribution d'un processus OSPF à un autre processus OSPF sur le même routeur, la mesure sera transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus vers un processus OSPF, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée. La valeur par défaut est 0.
- (Facultatif) match internal | external1 | external2 | NSSA external 1 | NSSA external 2 : pour les critères selon lesquels les routes OSPF sont redistribuées dans d'autres domaines de routage. Les choix sont les suivants :
  - internal : routes internes à un système autonome spécifique.
  - external 1 : routes externes au système autonome, mais importées dans BGP en tant que route externe OSPF de type 1.
  - external 2 : routes externes au système autonome, mais importées dans BGP en tant que route externe OSPF de type 2.
  - NSSA external 1 : routes externes au système autonome, mais importées dans BGP en tant que routes externes OSPF NSSA de type 1.
  - NSSA external 2 : routes externes au système autonome, mais importées dans BGP en tant que routes externes OSPF NSSA de type 2.
- (Facultatif) map-tag : l'identifiant d'une carte de routage configurée.

Remarque
Il faut examiner la carte de routage pour filtrer les réseaux à redistribuer. S'ils ne sont pas spécifiés, tous les réseaux sont redistribués.

Configurer les paramètres d'injection de route IPv6

Cette section décrit les étapes nécessaires pour définir les routes à injecter de manière conditionnelle dans la table de routage de BGP.

Procédure

Étape 1 Activez un processus de routage BGP, qui place l'ASA en mode de configuration de routeur :

router bgp autonomous-num

Exemple :

```
ciscoasa(config)# router bgp 2
```

Étape 2 Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

address-family ipv6 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv6 [unicast]
```

Étape 3 Configurez l'injection conditionnelle de routes pour injecter des routes plus précises dans une table de routage de BGP :

bgp inject-map inject-map exist-map exist-map [copy-attributes]

Exemple :

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map : le nom de la carte de routage qui spécifie les préfixes à injecter dans la table de routage de BGP locale.
- exist-map : le nom de la carte de routage contenant les préfixes que le locuteur BGP suivra.
- (Facultatif) copy-attributes : configure la route injectée pour hériter des attributs de la route agrégée.

Supervision BGP

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage BGP. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande. En outre, vous pouvez désactiver la journalisation des messages de modification de voisin et des messages d'avertissement de voisin.

Pour superviser diverses statistiques de routage BGP, saisissez l'une des commandes suivantes :

- **show bgp** [ip-address [mask [longer-prefixes [injected] | shorter-prefixes [length]]]| prefix-list name | route-map name]

  Affiche les entrées de la table de routage BGP.

- **show bgp** cidr-only

  Affiche les routes avec des masques réseau non naturels (c'est-à-dire le routage inter-domaine sans classe ou CIDR).

- **show bgp community community-number [exact-match][no-advertise][no-export]**

  Affiche les routes qui appartiennent aux communautés BGP spécifiées.

- **show bgp community-list community-list-name [exact-match]**

  Affiche les routes autorisées par la liste de communautés BGP.

- **show bgp filter-list** *access-list-number*

  Affiche les routes conformes à une liste de filtres spécifiée.

- **show bgp injected-paths**

  Affiche tous les chemins injectés dans la table de routage BGP.

- **show bgp ipv4 unicast**

  Affiche les entrées de la table de routage BGP d'IP version 4 (IPv4) pour les sessions de monodiffusion.

- show bgp ipv6 unicast

  Affiche les entrées de la table de routage du protocole de passerelle frontière (BGP) IPv6.

- show bgp ipv6 community

  Affiche les routes qui appartiennent aux communautés du protocole de passerelle frontière (BGP) IPv6 spécifiées.

- show bgp ipv6 community-list

  Affiche les routes autorisées par la liste de communautés du protocole de passerelle frontière (BGP) IPv6.

- show bgp ipv6 filter-list

  Affiche les routes conformes à une liste de filtres IPv6 spécifiée.

- show bgp ipv6 inconsistent-as

  Affiche les routes du protocole de passerelle frontière (BGP) IPv6 dont les systèmes autonomes sont incohérents.

- show bgp ipv6 neighbors

  Affiche des renseignements sur les connexions du protocole de passerelle frontière (BGP) IPv6 aux voisins.

- show bgp ipv6 paths

  Affiche tous les chemins du protocole de passerelle frontière (BGP) IPv6 dans la base de données.

- show bgp ipv6 prefix-list

Affiche les routes qui correspondent à une liste de préfixes.

- show bgp ipv6 quote-regexp

  Affiche les routes du protocole de passerelle frontière (BGP) IPv6 correspondant à l'expression régulière du chemin d'accès au système autonome sous la forme d'une chaîne de caractères entre guillemets.

- show bgp ipv6 regexp

  Affiche les routes du protocole de passerelle frontière (BGP) IPv6 correspondant à l'expression régulière du chemin d'accès au système autonome.

- show bgp ipv6 route-map

  Affiche les routes du protocole de passerelle frontière (BGP) IPv6 qui n'ont pas pu être installées dans la table de routage.

- show bgp ipv6 summary

  Affiche l'état de toutes les connexions du protocole de passerelle frontière (BGP) IPv6.

- show bgp neighbors ip_address

  Affiche des renseignements sur les connexions BGP et TCP à des voisins.

- show bgp paths [LINE]

  Affiche tous les chemins BGP dans la base de données.

- show bgp pending-prefixes

  Affiche les préfixes qui sont en attente de suppression.

- show bgp prefix-list prefix_list_name [WORD]

  Affiche les routes qui correspondent à une liste de préfixes spécifiée.

- show bgp regexp regexp

  Affiche les routes qui correspondent à l'expression régulière du chemin d'accès au système autonome.

- show bgp replication [index-group | ip-address]

  Affiche les statistiques de réplication de mise à jour pour les groupes de mise à jour du BGP.

- show bgp rib-failure

  Affiche les routes BGP qui n'ont pas pu être installées dans le tableau de la base d'information de routage (RIB).

- show bgp route-map map-name

  Affiche les entrées de la table de routage BGP, en fonction de la carte de routage spécifiée.

- show bgp summary

  Affiche l'état de toutes les connexions BGP.

- show bgp system-config

  Affiche la configuration BGP spécifique au contexte système en mode de contexte multiple.

  Cette commande est disponible dans tous les contextes utilisateur en mode de contexte multiple.

- show bgp update-group

  Affiche des renseignements sur les groupes de mise à jour du BGP.



Remarque Pour désactiver les messages du journal BGP, saisissez la commande **no bgp log-neighbor-changes** dans le mode de configuration du routeur. Cela désactive la journalisation des messages de modification de voisin. Saisissez cette commande en mode de configuration du routeur pour le processus de routage BGP. Par défaut, les modifications de voisins sont journalisées.

Exemple de BGP

Cet exemple montre comment activer et configurer BGPv4 avec différents processus facultatifs.

1. Définissez les conditions pour la redistribution des routes d'un protocole de routage vers un autre protocole de routage, ou activez le routage par politique :

```
ciscoasa(config)# route-map mymap2 permit 10
```

2. Redistribuez toutes les routes qui ont une adresse de route ou un paquet correspondant à une des listes d'accès spécifiées :

```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

3. Indiquez où obtenir les paquets qui transmettent une clause de correspondance d'une carte de routage pour le routage des politiques :

```
ciscoasa(config-route-map)# set ip next-hop peer address
```

4. Activez un processus de routage BGP à partir du mode de configuration global :

```
ciscoasa(config)# router bgp 2
```

5. Configurez un ID de routeur fixe pour le processus de routage du protocole BGP (Border Gateway Protocol) local dans le mode de configuration de la famille d'adresses :

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. Ajoutez une entrée au tableau de voisins BGP :

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

7. Appliquez une carte de routage aux routes entrantes ou sortantes :

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

8. Mettez à jour une interface en tant que source d'un voisin prenant en charge le protocole BGP :

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 update-source loop1
```

Cet exemple montre comment activer et configurer BGPv6 avec différents processus facultatifs.

1. Définissez les conditions pour la redistribution des routes d'un protocole de routage vers un autre protocole de routage, ou activez le routage par politique :

```
ciscoasa(config)# route-map mymap1 permit 10
```

2. Redistribuez toutes les routes qui ont une adresse de route ou un paquet correspondant à une des listes d'accès spécifiées :

```
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

3. Indiquez où obtenir les paquets qui transmettent une clause de correspondance d'une carte de routage pour le routage des politiques :

```
ciscoasa(config-route-map)# set ipv6 next-hop peer address
```

4. Activez un processus de routage BGP à partir du mode de configuration global :

```
ciscoasa(config)# router bgp 2
```

5. Configurez un ID de routeur fixe pour le processus de routage du protocole BGP (Border Gateway Protocol) local dans le mode de configuration de la famille d'adresses :

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. Passez en mode de configuration de famille d'adresses pour configurer une session de routage à l'aide des préfixes d'adresse IP standard version 6 (IPv6) :

```
address-family ipv6 [unicast]
```

7. Ajoutez une entrée au tableau de voisins BGP :

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 64600
```

8. Appliquez une carte de routage aux routes entrantes ou sortantes :

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 route-map mymap1 in
```

9. Mettez à jour une interface en tant que source d'un voisin prenant en charge le protocole BGP :

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 update-source loop1
```

Historique de BGP

Tableau 40 : Historique des fonctionnalités de BGP

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge BGP	9.2(1)	Une prise en charge a été ajoutée pour le routage des données, l'exécution de l'authentification, ainsi que la redistribution et la supervision des informations de routage à l'aide du protocole de passerelle frontière. Nous avons introduit les commandes suivantes : **router bgp, bgp maxas-limit, bgp log-neighbor-changes, bgp transport path-mtu-discovery, bgp fast-external-fallover, bgp enforce-first-as, bgp asnotation dot, timers bgp, bgp default local-preference, bgp always-compare-med, bgp bestpath compare-routerid, bgp deterministic-med, bgp bestpath med missing-as-worst, policy-list, match as-path, match community, match metric, match tag, as-path access-list, community-list, address-family ipv4, bgp router-id, distance bgp, table-map, bgp suppress-inactive, bgp redistribute-internal, bgp scan-time, bgp nexthop, aggregate-address, neighbor, bgp inject-map, show bgp, show bgp cidr-only, show bgp all community, show bgp all neighbors, show bgp community, show bgp community-list, show bgp filter-list, show bgp injected-paths, show bgp ipv4 unicast, show bgp neighbors, show bgp paths, show bgp pending-prefixes, show bgp prefix-list, show bgp regexp, show bgp replication, show bgp rib-failure, show bgp route-map, show bgp summary, show bgp system-config, show bgp update-group, clear route network, maximum-path, network.** Nous avons modifié les commandes suivantes : **show route**, **show route summary**, **show running-config router**, **clear config router**, **clear route all**, **timers lsa arrival**, **timers pacing**, **timers throttle**, **redistribute bgp**.
Prise en charge BGP pour la mise en grappe d'ASA	9.3(1)	Nous avons ajouté la prise en charge de la mise en grappe de niveau 2 et de niveau 3. Nous avons introduit la commande suivante : bgp router-id clusterpool
Prise en charge BGP pour la transmission sans interruption	9.3(1)	Nous avons ajouté la prise en charge de la transmission sans interruption. Nous avons introduit les commandes suivantes : bgp graceful-restart, neighbor ha-mode graceful-restart

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge BGP pour les cartes annoncées	9.3(1)	Nous avons ajouté la prise en charge des cartes annoncées BGPv4. Nous avons introduit la commande suivante : neighbor advertise-map
Prise en charge BGP pour IPv6	9.3(2)	Nous avons ajouté la prise en charge d'IPv6. Nous avons introduit les commandes suivantes : address-family ipv6, ipv6 prefix-list, ipv6 prefix-list description, ipv6 prefix-list sequence-number, match ipv6 next-hop, match ipv6 route-source, match ipv6- address prefix-list, set ipv6-address prefix -list, set ipv6 next-hop, set ipv6 next-hop peer-address Nous avons modifié la commande suivante : bgp router-id
Annonce de réseau IPv6 pour les préfixes délégués	9.6(2)	L'ASA prend désormais en charge le client de délégation de préfixe DHCPv6. L'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. Vous pouvez configurer le routeur BGP pour annoncer ces préfixes. Nous avons modifié la commande suivante : **network**
Prise en charge de l'interface de boucle avec retour pour le trafic BGP	9.18(2)	Vous pouvez utiliser une interface de boucle avec retour pour le trafic BGP. Commandes nouvelles/modifiées : **interface loopback**, **neighbor update-source**
Prise en charge du redémarrage progressif pour IPv6	9.19(1)	Nous avons ajouté la prise en charge du redémarrage progressif pour la famille d'adresses IPv6.



CHAPITRE 33

OSPF

Ce chapitre décrit comment configurer l'ASA pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de routage Open Shortest Path First (OSPF).

- À propos d'OSPF, à la page 1041
- Directives pour OSPF, à la page 1044
- Configurer le protocole OSPFv2, à la page 1047
- Configurer l'ID de routeur OSPFv2, à la page 1051
- Configurer les paquets Hello rapides OSPF, à la page 1052
- Personnaliser le protocole OSPFv2, à la page 1053
- Configurer le protocole OSPFv3, à la page 1069
- Configurer le redémarrage progressif, à la page 1090
- Exemple de protocole OSPFv2, à la page 1095
- Exemples de protocole OSPFv3, à la page 1097
- Supervision OSPF, à la page 1098
- Historique OSPF, à la page 1102

À propos d'OSPF

OSPF est un protocole de routage de passerelle intérieure qui utilise des états de liaison plutôt que des vecteurs de distance pour la sélection de chemin. OSPF propage des publicités d'état de liens plutôt que des mises à jour de la table de routage. Comme seuls les LSA sont échangés au lieu des tableaux de routage complets, les réseaux OSPF convergent plus rapidement que les réseaux IPS.

OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues. Chaque routeur d'une zone OSPF contient une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

Les avantages d'OSPF par rapport à RIP sont les suivants :

- Les mises à jour de la base de données d'états de liens OSPF sont envoyées moins fréquemment que les mises à jour RIP, et la base de données d'états de liens est mise à jour instantanément, plutôt que lentement, à mesure que les informations périmées expirent.
- Les décisions de routage sont basées sur le coût, qui est une indication du surdébit nécessaire pour envoyer des paquets sur une certaine interface. ASA calcule le coût d'une interface en fonction de la bande passante du lien plutôt que du nombre de sauts vers la destination. Le coût peut être configuré pour préciser les chemins privilégiés.

L'inconvénient des algorithmes du chemin le plus court d'abord est qu'ils nécessitent beaucoup de cycles du processeur et de mémoire.

L'ASA peut exécuter deux processus du protocole OSPF simultanément sur différents ensembles d'interfaces. Vous pourriez souhaiter exécuter deux processus si vous avez des interfaces qui utilisent les mêmes adresses IP (la NAT permet à ces interfaces de coexister, mais OSPF ne permet pas le chevauchement d'adresses). Ou vous pouvez exécuter un processus à l'intérieur et un autre à l'extérieur et redistribuer un sous-ensemble de routes entre les deux processus. De même, vous devrez peut-être séparer les adresses privées des adresses publiques.

Vous pouvez redistribuer les routages dans un processus de routage OSPF à partir d'un autre processus de routage OSPF, d'un processus de routage IP ou de routes statiques et connectées configurées sur des interfaces activées pour OSPF.

ASA prend en charge les fonctionnalités OSPF suivantes :

- Routages intra-zones, inter-zones et externes (type I et type II).
- Liens virtuels.
- Inondation de LSA.
- Authentification pour les paquets OSPF (authentification par mot de passe et authentification MD5).
- Configuration de ASA en tant que routeur désigné ou routeur de secours désigné L'ASA peut également être configuré comme un ABR.
- Zones tampons et zones tampons.
- Routeur de frontière de zone, filtrage LSA de type 3

OSPF prend en charge MD5 et l'authentification du voisin en texte clair. L'authentification doit être utilisée avec tous les protocoles de routage lorsque cela est possible, car la redistribution de routage entre OSPF et d'autres protocoles (comme RIP) peut être utilisée par les attaquants pour détourner des informations de routage.

Si la NAT est utilisée, si OSPF fonctionne sur des zones publiques et privées, et si le filtrage d'adresses est requis, vous devez exécuter deux processus OSPF, un pour les zones publiques et un pour les zones privées.

Un routeur qui a des interfaces dans plusieurs zones est appelé routeur de frontière de zone (ABR). Un routeur qui agit comme une passerelle pour redistribuer le trafic entre les routeurs utilisant OSPF et les routeurs utilisant d'autres protocoles de routage est appelé un routeur de frontière de système autonome (ASBR).

Un ABR utilise des LSA pour envoyer des informations sur les routes disponibles à d'autres routeurs OSPF. Le filtrage du LSA ABR de type 3 vous permet d'avoir des zones privée et publique distinctes, l'ASA agissant comme un ABR. Les LSA de type 3 (routes inter-zones) peuvent être filtrées d'une zone à une autre, ce qui vous permet d'utiliser la NAT et l'OSPF ensemble sans annoncer de réseaux privés.



Remarque Seuls les LSA de type 3 peuvent être filtrés. Si vous configurez l'ASA comme ASBR dans un réseau privé, il enverra des LSA de type 5 décrivant les réseaux privés, qui seront inondés à l'ensemble du système autonome, y compris les zones publiques.

Si la NAT est utilisée, mais OSPF n'est exécuté que dans les zones publiques, les routages vers les réseaux publics peuvent être redistribués à l'intérieur du réseau privé, soit par défaut, soit comme LSA externes de

type AS externes. Cependant, vous devez configurer des routes statiques pour les réseaux privés protégés par ASA. De plus, vous ne devez pas combiner réseaux publics et réseaux privés sur la même interface ASA.

Vous pouvez avoir deux processus de routage OSPF, un processus de routage RIP et un processus de routage EIGRP en même temps sur l'ASA.

Prise en charge OSPF pour les paquets Fast Hello

La prise en charge OSPF des paquets Hello rapides offre un moyen de configurer l'envoi de paquets Hello à des intervalles inférieurs à une seconde. Une telle configuration accélérerait la convergence dans un réseau OSPF (Open Shortest Path First).

Conditions préalables à la prise en charge d'OSPF pour les paquets Fast Hello

OSPF doit déjà être configuré dans le réseau ou configuré en même temps que la fonction de prise en charge OSPF des paquets Fast Hello.

À propos de la prise en charge OSPF pour les paquets Hello rapides

Les concepts clés liés à la prise en charge OSPF pour les paquets Fast Hello et aux avantages des paquets OSPF Fast Hello sont décrits ci-dessous :

Intervalle Hello et intervalle mort OSPF

Les paquets Hello OSPF sont des paquets qu'un processus OSPF envoie à ses voisins OSPF pour maintenir la connectivité avec ces derniers. Les paquets Hello sont envoyés à un intervalle configurable (en secondes). Les valeurs par défaut sont de 10 secondes pour une liaison Ethernet et de 30 secondes pour une liaison non diffusée. Les paquets Hello comprennent une liste de tous les voisins pour lesquels un paquet Hello a été reçu dans l'intervalle mort. L'intervalle mort est également un intervalle configurable (en secondes). Par défaut, il est quatre fois supérieur à la valeur de l'intervalle Hello. La valeur de tous les intervalles Hello doit être la même dans un réseau. De même, la valeur de tous les intervalles morts doit être la même dans un réseau.

Ces deux intervalles fonctionnent ensemble pour maintenir la connectivité en indiquant que la liaison est opérationnelle. Si un routeur ne reçoit pas de paquet Hello d'un voisin dans l'intervalle mort, il déclarera ce voisin en panne.

Paquets Fast Hello OSPF

Les paquets Hello OSPF rapides sont des paquets Hello envoyés à des intervalles de moins d'une seconde. Pour comprendre les paquets Hello rapides, vous devez déjà comprendre la relation entre les paquets Hello d'OSPF et l'intervalle mort. Consultez Intervalle Hello et intervalle mort OSPF, à la page 1043.

Les paquets OSPF fast Hello sont obtenus à l'aide de la commande ospf dead-interval. L'intervalle mort est défini à 1 seconde et la valeur Hello-multiplier est définie sur le nombre de paquets Hello que vous souhaitez envoyer pendant cette 1 seconde, fournissant ainsi des paquets Hello inférieurs à la seconde ou « rapides ».

Lorsque des paquets Hello rapides sont configurés sur l'interface, l'intervalle Hello annoncé dans les paquets Hello envoyés par cette interface est réglé à 0. L'intervalle Hello dans les paquets Hello reçus sur cette interface est ignoré.

L'intervalle mort doit être cohérent sur un segment, qu'il soit défini à 1 seconde (pour les paquets Hello rapides) ou à une autre valeur. Le multiplicateur Hello n'a pas besoin d'être le même pour tout le segment tant qu'au moins un paquet Hello est envoyé dans l'intervalle mort.

Avantages des paquets Fast Hello OSPF

L'avantage de la fonctionnalité OSPF Fast Hello Packets est que votre réseau OSPF connaîtra un temps de convergence plus rapide que sans les paquets rapides Hello. Cette fonctionnalité vous permet de détecter les voisins perdus en moins d'une seconde. Elle est particulièrement utile dans les segments de réseau local, où la perte de voisin peut ne pas être détectée par la couche physique et la couche de liaison de données de l'Open System Interconnection (OSI).

Différences d'implémentation entre OSPFv2 et OSPFv3

OSPFv3 n'est pas rétrocompatible avec OSPFv2. Pour utiliser OSPF en vue d'acheminer le trafic IPv4 et IPv6, vous devez exécuter simultanément OSPFv2 et OSPFv3. Ils coexistent, mais n'interagissent pas entre eux.

Les fonctionnalités supplémentaires fournies par OSPFv3 sont les suivantes :

- Traitement du protocole par liaison
- Suppression de la sémantique d'adressage.
- Ajout de la portée de submersion.
- Prise en charge de plusieurs instances par lien.
- Utilisation de l'adresse locale de lien IPv6 pour la découverte de voisin et d'autres fonctionnalités.
- Les LSA sont exprimées en tant que préfixe et longueur de préfixe.
- Ajout de deux types de LSA.
- Gestion des types de LSA inconnus
- Prise en charge de l'authentification par la norme IPsec ESP pour le trafic de protocole de routage OSPFv3, comme le spécifie la RFC 4552.

Directives pour OSPF

Directives relatives au mode contextuel

OSPFv2 prend en charge les modes à contexte unique et multiple.

- Les instances OSPFv2 ne peuvent pas former de contiguïtés entre elles dans les interfaces partagées car, par défaut, l'échange inter-contextes du trafic de multidiffusion n'est pas pris en charge sur les interfaces partagées. Cependant, vous pouvez utiliser la configuration de voisin statique sous la configuration de processus OSPFv2 sous le processus OSPFv2 pour faire apparaître le voisinage OSPFv2 sur une interface partagée.
- OSPFv2 inter-contexte sur des interfaces distinctes est pris en charge.

(Pour la topologie point à point) En mode de contexte multiple, vous pouvez configurer des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Pour une formation de contiguïté OSPF réussie, lorsque vous supprimez et reconfigurez OSPF sur une interface partagée, exécutez les commandes dans l'ordre suivant :

- Supprimez la configuration OSPF en utilisant `no router <ospf name>`, puis supprimez la configuration OSPF point à point de non-diffusion sur l'interface en utilisant `no ospf network point-to-point non-broadcast`.
- Lorsque vous reconfigurez OSPF sur l'interface partagée, configurez le routeur OSPF en utilisant `router <ospf name>`, puis configurez l'interface avec `ospf network point-to-point non-broadcast`.

OSPFv3 prend en charge le mode unique uniquement.

Directives d'authentification par chaîne de clé

OSPFv2 prend en charge l'authentification par chaîne de clés en mode unique et multiple, en modes physique et virtuel. Cependant, en mode multiple, vous pouvez configurer la chaîne de clés uniquement en mode contextuel.

- Les clés pivotantes ne s'appliquent qu'au protocole OSPFv2. L'authentification de zone OSPF avec chaîne de clé n'est pas prise en charge.
- L'authentification MD5 existante sans plage temporelle dans OSPFv2 est toujours prise en charge avec les nouvelles clés alternées.
- Bien que la plateforme prenne en charge les algorithmes cryptographiques SHA1 et MD5, seul l'algorithme cryptographique MD5 est utilisé pour l'authentification.

Directives sur le mode pare-feu

OSPF ne prend en charge que le mode pare-feu routé. OSPF ne prend pas en charge le mode de pare-feu transparent.

Directives Failover (basculement)

OSPFv2 et OSPFv3 prennent en charge le Failover (basculement) sans état.

Directives IPv6

- OSPFv2 ne prend pas en charge IPv6.
- OSPFv3 prend en charge IPv6.
- OSPFv3 utilise IPv6 pour l'authentification.
- L'ASA installe les routages OSPFv3 dans le RIB IPv6, à condition qu'il s'agisse du meilleur routage.
- Les paquets OSPFv3 peuvent être filtrés à l'aide des listes de contrôle d'accès IPv6 dans la commande **capture**.

Paquets Hello OSPFv3 et GRE

En règle générale, le trafic OSPF ne passe pas par le tunnel GRE. Lorsqu'OSPFv3 sur IPv6 est encapsulé à l'intérieur de GRE, la validation de l'en-tête IPv6 pour les vérifications de sécurité telles que la destination de multidiffusion échoue. Le paquet est abandonné en raison de la validation de vérification de sécurité implicite, car ce paquet a une multidiffusion IPv6 de destination.

Vous pouvez définir une règle de préfiltre pour contourner le trafic GRE. Cependant, avec la règle de préfiltre, les paquets internes ne seraient pas interrogés par le moteur d'inspection.

Directives de mise en grappe

- Le chiffrement OSPFv3 n'est pas pris en charge. Un message d'erreur s'affiche si vous essayez de configurer le chiffrement OSPFv3 dans un environnement de mise en grappe.
- En mode d'interface étendue, le routage dynamique n'est pas pris en charge sur les interfaces de gestion uniquement.
- En mode d'interface individuel, veillez à définir les unités de contrôle et de données comme des voisins OSPFv2 ou OSPFv3.
- En mode d'interface individuelle, les contiguïtés OSPFv2 ne peuvent être établies qu'entre deux contextes sur une interface partagée sur l'unité de contrôle. La configuration de voisins statiques est prise en charge uniquement sur les liaisons point à point; par conséquent, une seule instruction voisin est autorisée sur une interface.
- Lorsqu'un changement de rôle de contrôle se produit dans la grappe, le comportement suivant se produit :
  - En mode d'interface étendue, le processus du routeur est actif uniquement sur l'unité de contrôle et est à l'état suspendu sur les unités de données. Chaque unité de grappe a le même ID de routeur, car la configuration a été synchronisée à partir de l'unité de contrôle. Par conséquent, un routeur voisin ne remarque aucun changement dans l'ID de routeur de la grappe lors d'un changement de rôle.
  - En mode d'interface individuelle, le processus du routeur est actif sur toutes les unités de la grappe. Chaque unité de grappe choisit son propre ID de routeur dans l'ensemble de grappes configuré. Une modification du rôle de contrôle dans la grappe ne modifie en rien la topologie de routage.

Commutation multiprotocole par étiquette (MPLS) et directives OSPF

Lorsqu'un routeur configuré pour MPLS envoie des paquets de mise à jour d'état de liaison (LS) qui contiennent des publicités d'état de liaison (LSA) de type 10 couvrantes qui comprennent un en-tête MPLS, l'authentification échoue et le périphérique abandonne en mode silencieux les paquets de mise à jour plutôt que d'en accuser réception. Finalement, le routeur homologue mettra fin à la relation de voisin, car il n'a reçu aucun accusé de réception.

Désactivez la capacité d'opacité sur l'ASA pour vous assurer que la relation de voisin reste stable :

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```



Remarque Les modèles Firepower 4100/9300 peuvent avoir une latence élevée lors de l'utilisation de MPLS, car ils n'ont pas suffisamment d'équilibrage de la charge sur plusieurs files d'attente de réception.

Directives de redistribution de routage

- La redistribution des cartes de routage avec la liste de préfixes IPv4 sur OSPFv2 est prise en charge. Toutefois, la redistribution des cartes de routage avec la liste de préfixes IPv6 sur OSPFv3 n'est pas prise en charge. Utilisez une liste d'accès dans la carte de routage sur OSPF pour la redistribution.

- Lorsqu'OSPF est configuré sur un périphérique qui fait partie du réseau EIGRP ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser la voie de routage (le protocole EIGRP ne prend pas encore en charge la balise de routage).

  Lors de la redistribution d'OSPF dans EIGRP et d'EIGRP dans OSPF, une boucle de routage se produit lorsqu'il y a une panne sur l'une des liaisons ou des interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

Directives supplémentaires

- OSPFv2 et OSPFv3 prennent en charge plusieurs instances sur une interface.
- OSPFv3 prend en charge le chiffrement par le biais des en-têtes ESP dans un environnement sans grappe.
- OSPFv3 prend en charge le chiffrement sans charge utile.
- OSPFv2 prend en charge les mécanismes de redémarrages progressifs NSF de Cisco et IETF NSF tels que définis dans les RFC 4811, 4812 et 3623 respectivement.
- OSPFv3 prend en charge le mécanisme de redémarrage progressif tel que défini dans la RFC 5187.
- Il y a une limite au nombre de routages intra-zone (type 1) qui peuvent être distribués. Pour ces routes, un seul LSA de type 1 contient tous les préfixes. Comme le système a une limite de 35 Ko pour la taille des paquets, un paquet de 3 000 routages dépasse la limite. Considérez 2900 routes de type 1 comme le nombre maximal pris en charge.
- Pour éviter les oscillations de contiguïté dues aux mises à jour de routage abandonnées si la mise à jour de routage est supérieure à la MTU minimale sur le lien, configurez la même MTU sur les interfaces des deux côtés du lien.
- L'ASA virtuel ne peut pas utiliser les protocoles de routage interne dynamique comme EIGRP et OSPF en raison de la nature du routage dans le nuage Azure. La table de routage effective détermine le saut suivant, que le client virtuel ait ou non une route statique/dynamique configurée.

  Actuellement, vous ne pouvez pas afficher la table de routage effective ou la table de routage du système.
- OSPFv3 abandonne la mise à jour LS si la taille des paquets dépasse 8190. Par conséquent, le voisinage est interrompu. Ainsi, configurez le commutateur avec la commande « ospfv3 mtu-ignore » pour éviter la fin du voisinage.

Configurer le protocole OSPFv2

Cette section décrit comment activer un processus OSPFv2 sur l'ASA.

Après avoir activé le protocole OSPFv2, vous devez définir une carte de routage. Pour en savoir plus, consultez Définir une carte de routage, à la page 983. Ensuite, vous générez une route par défaut. Pour en savoir plus, consultez Configurer une route statique, à la page 956.

Après avoir défini une carte de routage pour le processus OSPFv2, vous pouvez la personnaliser selon vos besoins particuliers. Pour savoir comment personnaliser le processus OSPFv2 sur l'ASA, consultez Personnaliser le protocole OSPFv2, à la page 1053.

Pour activer le protocole OSPFv2, vous devez créer un processus de routage OSPFv2, spécifier la plage d'adresses IP associées au processus de routage, puis attribuer les ID de zone associés à cette plage d'adresses IP.

Vous pouvez activer jusqu'à deux instances de processus OSPFv2. Chaque processus OSPFv2 a ses propres zones et réseaux associés.

Pour activer le processus OSPFv2, procédez comme suit.

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

S'il n'y a qu'un seul processus OSPF activé sur l'ASA, ce processus est sélectionné par défaut. Vous ne pouvez pas modifier l'ID de processus OSPF lors de la modification d'une zone existante.

Étape 2 Définissez les adresses IP sur lesquelles l'OSPF s'exécute et l'ID de zone pour cette interface :

network *ip_address mask* **area** *area_id*

Exemple :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

Lors de l'ajout d'une nouvelle zone, saisissez l'ID de zone. Vous pouvez spécifier l'ID de zone sous la forme d'un nombre décimal ou d'une adresse IP. Les valeurs décimales valides vont de 0 à 4294967295. Vous ne pouvez pas modifier l'ID de zone lors de la modification d'une zone existante.

Configurer une chaîne de clés pour l'authentification

Pour améliorer la sécurité et la protection des données des périphériques, vous pouvez activer des clés changeantes pour l'authentification des homologues IGP. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active. Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Cette section décrit comment créer une chaîne de clés pour l'authentification des homologues OSPF. Après avoir configuré un objet de chaîne de clés, vous pouvez l'utiliser pour définir l'authentification OSPFv2 pour une interface et pour une liaison virtuelle. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie. Pour savoir comment définir l'authentification pour une interface, consultez Configurer les paramètres d'interface OSPFv2, à la page 1057.

Pour configurer une chaîne de clés, procédez comme suit :

Procédure

Étape 1 Configurez une chaîne de clés avec un nom :

key chain*key-chain-name*

Exemple :

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)#
```

Vous pouvez maintenant définir les paramètres associés à la chaîne de clés.

Étape 2 Configurez l'identifiant de la chaîne de clés :

key*key-id*

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Exemple :

```
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)#
```

Étape 3 Configurez la clé ou le mot de passe de la chaîne de clés :

key-string [**0** | **8**] *key-string-text*

- Utilisez **0** pour indiquer qu'un mot de passe non chiffré suit, comme le montre l'exemple.
- Utilisez **8** pour indiquer qu'un mot de passe chiffré suit.
- La longueur maximale du mot de passe peut être de 80 caractères.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Exemple :

```
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)#
```

Étape 4 Configurez l'algorithme cryptographique pour la chaîne de clés :

cryptographic-algorithm*md5*

Vous devez fournir l'algorithme d'authentification cryptographique. Bien que la plateforme prenne en charge SHA1 et MD5, seul MD5 est pris en charge pour la gestion de la chaîne de clés.

Exemple :

```
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)#
```

Étape 5 (Facultatif) Configurez les paramètres de durée de vie de la chaîne de clés :

accept-lifetime [**local** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

send-lifetime [**ocal** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

Vous pouvez spécifier l'intervalle de temps nécessaire pour que le périphérique accepte ou envoie la clé lors de l'échange de clés avec un autre périphérique. L'heure de fin peut correspondre à la durée ou à l'heure absolue à laquelle la durée de vie de l'acceptation/envoi prend fin, ou être infinie.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie.

Exemple :

```
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite
ciscoasa(config-keychain-key)#
```

Vous pouvez utiliser la commande **show key chain** pour afficher la configuration de la chaîne de clés de démarrage sur le périphérique; **show run key chain** pour afficher la configuration de la chaîne de clés qui est actuellement en cours d'exécution sur le périphérique.

```
ciscoasa# show key chain
Key-chain CHAIN2:
    key 1 -- text "KEY1CHAIN2"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
  * key 2 -- text "(unset)"
        accept lifetime (11:00:12 UTC Sep 1 2018) - (11:12:12 UTC Sep 1 2018)
        send lifetime (always valid) - (always valid) [valid now]
Key-chain CHAIN1:
    key 1 -- text "CHAIN1KEY1STRING"
        accept lifetime (11:22:33 UTC Sep 1 2018) - (-1 seconds)
        send lifetime (always valid) - (always valid) [valid now]
ciscoasa#
```

```
ciscoasa# sh run key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
```

```
  cryptographic-algorithm md5
ciscoasa# sh run key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

Prochaine étape

Vous pouvez maintenant appliquer la chaîne de clés configurée pour définir l'authentification OSPFv2 pour une interface.

- Configurer les paramètres d'interface OSPFv2, à la page 1057

Configurer l'ID de routeur OSPFv2

L'ID de routeur OSPF est utilisé pour identifier un appareil spécifique dans une base de données OSPF. Deux routeurs d'un système OSPF ne peuvent pas avoir le même ID de routeur.

Si un ID de routeur n'est pas configuré manuellement dans le processus de routage OSPF, le routeur configurera automatiquement un ID de routeur déterminé à partir de l'adresse IP la plus élevée d'une interface active. Lors de la configuration d'un ID de routeur, les voisins ne seront pas mis à jour automatiquement jusqu'à ce que le routeur ait échoué ou que le processus OSPF ait été effacé et que la relation de voisin ait été rétablie.

Configurer manuellement l'ID de routeur OSPF

Cette section décrit comment configurer manuellement l'ID de routeur dans le processus OSPFv2 sur l'ASA.

Procédure

Étape 1 Pour utiliser un ID de routeur fixe, utilisez la commande **router-id**.

router-id *ip-address*

Exemple :

```
ciscoasa(config-router)# router-id 193.168.3.3
```

Étape 2 Pour revenir au comportement précédent de l'ID de routeur OSPF, utilisez la commande **no router-id**.

no router-id *ip-address*

Exemple :

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

Comportement de l'ID de routeur lors de la migration

Lors de la migration de la configuration OSPF d'un ASA, par exemple ASA 1 vers un autre ASA, par exemple l'ASA 2, le comportement suivant est observé en matière de sélection de l'ID du routeur :

1. L'ASA 2 n'utilise aucune adresse IP pour l'ID de routeur OSPF lorsque toutes les interfaces sont en mode d'arrêt. Les possibilités de configuration de l'ID de routeur lorsque toutes les interfaces sont à l'état « arrêt admin » ou en mode d'arrêt sont les suivantes :
   - Si l'ASA 2 n'a pas encore d'ID de routeur configuré, vous verrez ce message :

     `%OSPF: Router process 1 is not running, please configure a router-id` (% OSPF : le processus de routeur 1 n'est pas en cours d'exécution, veuillez configurer un identifiant de routeur)

     Après le déploiement de la première interface, l'ASA 2 utilisera l'adresse IP de cette interface comme ID de routeur.
   - Si l'ASA 2 a déjà configuré l'ID de routeur et que toutes les interfaces étaient à l'état « arrêt admin » lorsque la commande « no router-id » a été exécutée, l'ASA 2 utilisera l'ancien ID de routeur. L'ASA 2 utilise l'ancien ID de routeur, même si les adresses IP de l'interface créée sont modifiées, jusqu'à ce que la commande « clear ospf process » soit émise.
2. L'ASA 2 utilise un nouvel ID de routeur, alors que l'ASA 2 avait déjà configuré l'ID de routeur et qu'au moins une des interfaces n'était pas à l'état « arrêt admin » ou en mode d'arrêt lorsque la commande « no router-id » a été émise. L'ASA 2 utilisera le nouvel ID de routeur de l'adresse IP des interfaces même lorsque les interfaces sont à l'état « arrêt/arrêt ».

Configurer les paquets Hello rapides OSPF

Cette section explique comment configurer les paquets OSPF Hello rapides.

Procédure

Étape 1 Configurez une interface :

interface *port-channel number*

Exemple :

```
ciscoasa(config)# interface port-channel 10
```

L'argument *number* indique le numéro de l'interface de canal de port.

Étape 2 Définissez l'intervalle pendant lequel au moins un paquet Hello doit être reçu, sinon le voisin est considéré comme hors service :

ospf dead-interval minimal hello-multiplier *no.of times*

Exemple :

```
ciscoasa(config-if)# ospf dead-interval minimal hell0-multiplier 5
```

```
ciscoasa
```

L'argument no. of times indique le nombre de paquets Hello à envoyer chaque seconde. Les valeurs valides sont comprises entre 3 et 20.

Dans cet exemple, la prise en charge OSPF pour les paquets Hello rapides est activée en spécifiant le mot clé minimal et le mot clé hello-multiplier ainsi que sa valeur. Comme le multiplicateur est défini sur 5, cinq paquets Hello seront envoyés chaque seconde.

Personnaliser le protocole OSPFv2

Cette section explique comment personnaliser les processus OSPFv2.

Redistribuer les routes dans OSPFv2

L'ASA peut contrôler la redistribution des routes entre les processus de routage OSPFv2.

Remarque Si vous souhaitez redistribuer une route en définissant quelles routes du protocole de routage spécifié peuvent être redistribuées dans le processus de routage cible, vous devez d'abord générer une route par défaut. Consultez Configurer une route statique, à la page 956, puis définissez une carte de routage en fonction de Définir une carte de routage, à la page 983.

Pour redistribuer les routes statiques, connectées, RIP ou OSPFv2 dans un processus OSPFv2, procédez comme suit :

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Redistribuez les routes connectées dans le processus de routage OSPF :

redistribute connected [[**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# redistribute connected 5 type-1 route-map-practice
```

Étape 3 Redistribuez les routes statiques dans le processus de routage OSPF :

redistribute static [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# redistribute static subnets
```

Cette commande transmettra toutes les routes statiques à l'OSPF. Pour redistribuer les routes statiques sélectives, assurez-vous de créer une liste d'accès avec la route statique, puis de l'inclure dans une carte de routage :

Exemple :

```
ciscoasa(config)# ip access-list extended R1_Loopback
ciscoasa(config-ext-nacl)#permit ip host 1.1.1.1 any
ciscoasa(config-ext-nacl)#exit

ciscoasa(config)#route-map Permit_to_Distribute
ciscoasa(config-route-map)#match ip address R1_Loopback
ciscoasa(config-route-map)#exit
```

Après avoir créé la carte de routage, incluez-la dans la commande de redistribution comme suit :

Exemple :

```
ciscoasa(config)#router ospf 2
ciscoasa(config-router)#redistribute static subnets route-map Permit_to_Distribute
```

Étape 4 Redistribuez les routes d'un processus de routage OSPF dans un autre processus de routage OSPF :

redistribute ospf pid [**match {internal** | **external** [**1** | **2]** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

Vous pouvez utiliser les options **match** dans cette commande pour faire correspondre et définir les propriétés du routage, ou vous pouvez utiliser une carte de routage. L'option **subnets** n'a pas d'équivalents dans la commande **route-map**. Si vous utilisez à la fois une carte de routage et les options **match** dans la commande **redistribute**, elles doivent correspondre.

L'exemple montre la redistribution des routes du processus OSPF 1 vers le processus OSPF 2 en faisant correspondre les routes avec une mesure égale à 1. L'ASA redistribue ces routes en tant que LSA externes avec une mesure de 5 et un type de mesure de type 1.

Étape 5 Redistribuez les routes d'un processus de routage RIP dans le processus de routage OSPF :

redistribute rip [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# redistribute rip 5
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

Étape 6 Redistribuez les routes d'un processus de routage EIGRP dans le processus de routage OSPF :

redistribute eigrp as-num [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# redistribute eigrp 2
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

Configurer la synthèse des routes lors de la redistribution des routes dans OSPFv2

Lorsque les routages d'autres protocoles sont redistribués dans OSPF, chaque routage est annoncée individuellement dans un LSA externe. Cependant, vous pouvez configurer l'ASA pour annoncer une seule route pour toutes les routes redistribuées qui sont incluses pour une adresse et un masque réseau spécifiés. Cette configuration diminue la taille de la base de données d'états de liaison OSPF.

Les routes qui correspondent à la paire de masques d'adresses IP spécifiées peuvent être supprimées. La valeur de balise peut être utilisée comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Ajouter une adresse sommaire de route

Pour configurer l'annonce du logiciel sur une route récapitulative pour toutes les routes redistribuées incluses pour une adresse réseau et un masque, procédez comme suit :

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez l'adresse sommaire :

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

Exemple :

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

Dans cet exemple, l'adresse sommaire 10.1.0.0 comprend les adresses 10.1.1.0, 10.1.2.0, 10.1.3.0, etc. Seule l'adresse 10.1.0.0 est annoncée dans une annonce d'état de liaison externe.

Configurer la synthèse des routes entre les zones OSPFv2

La synthèse du routage est le regroupement d'adresses annoncées. Cette fonctionnalité permet d'annoncer une seule route récapitulative à d'autres zones par un routeur de délimitation de zone. Dans OSPF, un routeur de délimitation de zone annonce les réseaux d'une zone dans une autre zone. Si les numéros de réseau d'une zone sont affectés de manière à ce qu'ils soient contigus, vous pouvez configurer le routeur de délimitation de zone pour annoncer une route récapitulative qui inclut tous les réseaux individuels de la zone qui entrent dans la plage spécifiée.

Pour définir une plage d'adresses pour la synthèse du routage, procédez comme suit :

Procédure

Étape 1 Créez un processus de routage OSPF et entrez en mode de configuration du routeur pour ce processus OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il peut s'agir de n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez la plage d'adresses :

area *area-id* range *ip-address mask* [**advertise** | **not-advertise**]

Exemple :

```
ciscoasa(config-rtr)# area 17 range 12.1.0.0 255.255.0.0
```

Dans cet exemple, la plage d'adresses est définie entre les zones OSPF.

Configurer les paramètres d'interface OSPFv2

Vous pouvez modifier certains paramètres OSPFv2 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : **ospf hello-interval**, **ospf dead-interval** et **ospf authentication-key**. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Pour configurer les paramètres d'interface OSPFv2, procédez comme suit :

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf*process-id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez les adresses IP sur lesquelles l'OSPF s'exécute et l'ID de zone pour cette interface :

network*ip-address mask***area***area-id*

Exemple :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

Étape 3 Entrez le mode de configuration d'interface :

interface*interface-name*

Exemple :

```
ciscoasa(config)# interface my_interface
```

Étape 4 Spécifiez le type d'authentification pour une interface :

ospf authentication [**key-chain** *key-chain-name* | **message-digest** | **null**]

Fournissez le nom de la chaîne de clés configurée. Pour en savoir plus sur la configuration de la chaîne de clés, consultez Configurer une chaîne de clés pour l'authentification, à la page 1048

Exemple :

```
ciscoasa(config-interface)# ospf authentication message-digest
```

Étape 5 Attribuez un mot de passe à utiliser par les routeurs OSPF voisins sur un segment de réseau qui utilise l'authentification par mot de passe simple OSPF :

ospf authentication-key*key*

Exemple :

```
ciscoasa(config-interface)# ospf authentication-key cisco
```

L'argument *key* peut être n'importe quelle chaîne continue de caractères d'une longueur maximale de 8 octets.

Le mot de passe créé par cette commande est utilisé comme clé qui est insérée directement dans l'en-tête OSPF lorsque le logiciel ASA génère les paquets de protocole de routage. Un mot de passe distinct peut être attribué à chaque réseau par interface. Tous les routeurs voisins sur le même réseau doivent avoir le même mot de passe pour pouvoir échanger des renseignements OSPF.

Étape 6 Spécifiez explicitement le coût d'envoi d'un paquet sur une interface OSPF :

ospf cost*cost*

Exemple :

```
ciscoasa(config-interface)# ospf cost 20
```

Le *coût* est un entier compris entre 1 et 65 535.

Dans cet exemple, le coût est défini sur 20.

Étape 7 Définissez le nombre de secondes qu'un appareil doit attendre avant de déclarer un routeur OSPF voisin parce qu'il n'a pas reçu de paquet Hello :

ospf dead-interval*seconds*

Exemple :

```
ciscoasa(config-interface)# ospf dead-interval 40
```

La valeur doit être la même pour tous les nœuds du réseau.

Étape 8 Spécifiez la durée entre les paquets Hello que l'ASA envoie sur une interface OSPF :

ospf hello-interval*seconds*

Exemple :

```
ciscoasa(config-interface)# ospf hello-interval 10
```

La valeur doit être la même pour tous les nœuds du réseau.

Étape 9 Activez l'authentification MD5 OSPF :

ospf message-digest-key*key-id***md5***key*

Exemple :

```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

Les valeurs d'argument suivantes peuvent être définies :

key-id : un identifiant compris entre 1 et 255.

key : un mot de passe alphanumérique de 16 octets maximum.

Généralement, une clé par interface est utilisée pour générer des informations d'authentification lors de l'envoi de paquets et pour authentifier les paquets entrants. Le même identifiant de clé sur le routeur voisin doit avoir la même valeur de clé.

Nous vous conseillons de ne pas conserver plus d'une clé par interface. Chaque fois que vous ajoutez une nouvelle clé, vous devez supprimer l'ancienne clé pour empêcher le système local de continuer à communiquer avec un système malveillant qui connaît l'ancienne clé. La suppression de l'ancienne clé réduit également le surdébit lors du renouvellement.

Étape 10 Définissez la priorité pour aider à déterminer le routeur désigné OSPF pour un réseau :

ospf priority *number-value*

Exemple :

```
ciscoasa(config-interface)# ospf priority 20
```

L'argument *number_value* varie de 0 à 255.

En mode de contexte multiple, pour les interfaces partagées, spécifiez 0 pour vous assurer que le périphérique ne devienne pas le routeur désigné. Les instances OSPFv2 ne peuvent pas former de contiguïtés entre elles sur les interfaces partagées.

Étape 11 Spécifiez le nombre de secondes entre les retransmissions de LSA pour les contiguïtés appartenant à une interface OSPF :

ospf retransmit-interval*number-value*

Exemple :

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

La valeur pour *seconds* doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. La plage est comprise entre 1 et 8 192 secondes. La valeur par défaut est de 5 secondes.

Étape 12 Définissez le nombre estimé de secondes nécessaires pour envoyer un paquet de mise à jour d'état de liaison sur une interface OSPF :

ospf transmit-delay*seconds*

Exemple :

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

La valeur *seconds* varie de 1 à 8 192 secondes. La valeur par défaut est de 1 seconde.

Étape 13 Définissez le nombre de paquets Hello envoyés pendant 1 seconde :

ospf dead-interval minimal hello-interval multiplier*nombre entier*

Exemple :

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

Les valeurs valides sont des entiers compris entre 3 et 20.

Étape 14 Spécifiez l'interface comme réseau point à point sans diffusion :

ospf network point-to-point non-broadcast

Exemple :

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```

Lorsque vous désignez une interface comme point à point et sans diffusion, vous devez définir manuellement le voisin OSPF; la découverte dynamique de voisin n'est pas possible. Consultez Définir les voisins OSPFv2 statiques, à la page 1064 pour de plus amples renseignements. En outre, vous ne pouvez définir qu'un seul voisin OSPF sur cette interface.

Configurer les paramètres de zone OSPFv2

Vous pouvez configurer plusieurs paramètres de zone OSPF. Ces paramètres de zone (indiqués dans la liste des tâches suivante) comprennent la définition de l'authentification, la définition des zones tampons et l'affectation de coûts spécifiques à la route récapitulative par défaut. L'authentification offre une protection par mot de passe contre l'accès non autorisé à une zone.

Les zones tampons sont des zones dans lesquelles les informations sur les routages externes ne sont pas envoyées. Au lieu de cela, une route externe par défaut est générée par l'ABR dans la zone tampon pour les destinations externes au système autonome. Pour tirer parti de la prise en charge de la zone tampon OSPF, le routage par défaut doit être utilisé dans la zone tampon. Pour réduire davantage le nombre de LSA envoyés dans une zone tampon, vous pouvez utiliser le mot clé **no-summary** de la commande **area stub** sur l'ABR pour l'empêcher d'envoyer une annonce de liaison récapitulative (LSA type 3) dans la zone tampon.

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Activez l'authentification pour une zone OSPF :

area *area-id* authentication

Exemple :

```
ciscoasa(config-rtr)# area 0 authentication
```

Étape 3 Activez l'authentification MD5 pour une zone OSPF :

area *area-id* authentication message-digest

Exemple :

```
ciscoasa(config-rtr)# area 0 authentication message-digest
```

Configurer les règles de filtre OSPFv2

Utilisez la procédure suivante pour filtrer les routes ou les réseaux reçus ou transmis dans les mises à jour OSPF.

Procédure

Étape 1 Activez un processus de routage OSPF et passez en mode de configuration du routeur :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

Étape 2 Filtrez les routes ou les réseaux reçus dans les mises à jour OSPF entrantes ou annoncés dans les mises à jour OSPF sortantes :

distribute-list *acl-number* **in** [**interface** *ifname*]

distribute-list *acl-number* **out** [*protocol process-number* | **connected** | **static**]

L'argument *acl-number* spécifie le numéro de la liste d'accès IP. La liste d'accès définit les réseaux à recevoir et ceux à supprimer dans les mises à jour de routage.

Pour appliquer le filtre aux mises à jour entrantes, spécifiez **in**. Vous pouvez éventuellement définir une interface pour limiter le filtre aux mises à jour reçues sur cette interface.

Pour appliquer le filtre aux mises à jour sortantes, spécifiez **out**. Vous pouvez éventuellement spécifier un protocole (**bgp**, **eigrp**, **ospf** ou **rip**) avec un numéro de processus (à l'exception du protocole RIP) à appliquer

à la liste de distribution. Vous pouvez également filtrer selon que les homologues et les réseaux ont été appris par les routes **connected** ou **static**.

Exemple :

```
ciscoasa(config-rtr)# distribute-list ExampleAcl in interface inside
```

Configurer une NSSA OSPFv2

La mise en œuvre du protocole OSPFv2 d'une zone NSSA est similaire à une zone tampon OSPFv2. NSSA n'inonde pas les LSA externes de type 5 du cœur vers la zone, mais il peut importer des routes externes du système autonome de manière limitée dans la zone.

NSSA importe des routes externes du système autonome de type 7 dans une zone NSSA par redistribution. Ces LSA de type 7 sont traduites en LSA de type 5 par les ABR de NSSA, qui sont inondés dans tout le domaine de routage. La synthèse et le filtrage sont pris en charge pendant la traduction.

Vous pouvez simplifier l'administration si vous êtes un FAI ou un administrateur réseau qui doit connecter un site central à l'aide du protocole OSPFv2 à un site distant qui utilise un protocole de routage différent avec NSSA.

Avant la mise en œuvre de NSSA, la connexion entre le routeur de frontière du site d'entreprise et le routeur distant ne pouvait pas être exécutée en tant que zone tampon OSPFv2, car les routes du site distant ne pourraient pas être redistribuées dans la zone tampon, et deux protocoles de routage devaient être maintenus. Un protocole simple comme RIP était généralement exécuté et gérait la redistribution. Avec NSSA, vous pouvez étendre le protocole OSPFv2 pour couvrir la connexion à distance en définissant la zone entre le routeur d'entreprise et le routeur distant en tant que NSSA.

Veuillez consulter les lignes directrices suivantes avant d'utiliser cette fonctionnalité :

- Vous pouvez définir une route par défaut de type 7 qui peut être utilisée pour atteindre des destinations externes. Une fois configuré, le routeur génère une valeur par défaut de type 7 dans le NSSA ou le routeur de limite de zone NSSA.
- Tous les routeurs d'une même zone doivent convenir que la zone est NSSA; sinon, les routeurs ne peuvent pas communiquer entre eux.

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il peut s'agir de n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez une zone NSSA :

area *area-id* nssa [**no-redistribution**] [**default-information-originate**]

Exemple :

```
ciscoasa(config-rtr)# area 0 nssa
```

Étape 3 Définissez l'adresse sommaire et contribuez à réduire la taille de la table de routage :

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

Exemple :

```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

L'utilisation de cette commande pour OSPF amène un ASBR OSPF à annoncer une route externe en tant qu'agrégat pour toutes les routes redistribuées qui sont couvertes par l'adresse.

Dans cet exemple, l'adresse sommaire 10.1.0.0 comprend les adresses 10.1.1.0, 10.1.2.0, 10.1.3.0, etc. Seule l'adresse 10.1.0.0 est annoncée dans une annonce d'état de liaison externe.

Remarque
OSPF ne prend pas en charge l'adresse récapitulative 0.0.0.0 0.0.0.0.

Configurer un ensemble d'adresses IP pour la mise en grappe (OSPFv2 et OSPFv3)

Vous pouvez attribuer une plage d'adresses IPv4 pour le regroupement de grappes d'ID de routeur si vous utilisez la mise en grappe d'interfaces individuelles.

Pour attribuer une plage d'adresses IPv4 à l'ensemble de grappes d'ID de routeur dans la mise en grappe d'interfaces individuelles pour les protocoles OSPFv2 et OSPFv3, saisissez la commande suivante :

Procédure

Spécifiez l'ensemble de grappes d'ID de routeur pour la mise en grappe d'interfaces individuelles :

router-id cluster-pool hostname | A.B.C.D ip_pool

Exemple :

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
hostname(config-rtr)# log-adj-changes
```

Le mot clé **cluster-pool** permet la configuration d'un ensemble d'adresses IP lorsque la mise en grappe d'interfaces individuelles est configurée. Le mot clé **hostname** | **A.B.C.D.** spécifie l'ID du routeur OSPF pour ce processus OSPF. L'argument *ip_pool* spécifie le nom de l'ensemble d'adresses IP.

Remarque
Si vous utilisez la mise en grappe, vous n'avez pas besoin de spécifier d'ensemble d'adresses IP pour l'ID de routeur. Si vous ne configurez pas d'ensemble d'adresses IP, l'ASA utilise l'ID de routeur généré automatiquement.

Définir les voisins OSPFv2 statiques

Vous devez définir des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv2 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Avant de commencer, vous devez créer une route statique vers le voisin OSPFv2. Consultez Configurer une route statique, à la page 956 pour en savoir plus sur la création des routes statiques.

Procédure

Étape 1 Créez un processus de routage OSPFv2 :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez le voisinage OSPFv2 :

neighbor *addr* [**interface** if_name]

Exemple :

```
ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]
```

L'argument *addr* est l'adresse IP du voisin OSPFv2. L'argument *if_name* est l'interface utilisée pour communiquer avec le voisin. Si le voisin OSPFv2 ne se trouve pas sur le même réseau que l'une des interfaces connectées directement, vous devez préciser l'interface.

Configurer les minuteries de calcul de routage

Vous pouvez configurer le délai entre le moment où le protocole OSPFv2 reçoit une modification de topologie et le moment où il démarre un calcul SPF. Vous pouvez également configurer le délai de rétention entre deux calculs SPF consécutifs.

Procédure

Étape 1 Créez un processus de routage OSPFv2 :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez les minuteries de calcul de routage :

timers throttle spf *spf-start spf-hold spf-maximum*

Exemple :

```
ciscoasa(config-router)# timers throttle spf 500 500 600
```

L'argument *sf-start* est le délai (en millisecondes) entre le moment où OSPF reçoit une modification de topologie et le moment où il démarre un calcul SPF. Il peut s'agir d'un entier compris entre 0 et 600 000.

L'argument *spf-hold* est le temps minimal (en millisecondes) entre deux calculs SPF consécutifs. Il peut s'agir d'un entier compris entre 0 et 600 000.

L'argument spf-maximum est le temps maximal (en millisecondes) entre deux calculs SPF consécutifs. Il peut s'agir d'un entier de 0 à 600 000.

Journaliser les voisins en hausse ou en baisse

Par défaut, un message de journal système est généré lorsqu'un voisin OSPFv2 redevient disponible ou tombe en panne.

Configurez la commande **log-adj-changes** si vous souhaitez connaître l'augmentation ou la baisse des voisins OSPFv2 sans activer la commande **debug ospf adjacency**. La commande **log-adj-changes** fournit une vue de niveau supérieur de la relation avec les homologues avec moins de résultats. Configurez la commande **log-adj-changes detail** si vous souhaitez voir les messages pour chaque changement d'état.

Procédure

Étape 1 Créez un processus de routage OSPFv2 :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez la journalisation pour les voisins ascendants ou descendants :

log-adj-changes [**detail**]

Configurer une chaîne de clés pour l'authentification

Pour améliorer la sécurité et la protection des données des périphériques, vous pouvez activer des clés changeantes pour l'authentification des homologues IGP. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active. Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Cette section décrit comment créer une chaîne de clés pour l'authentification des homologues OSPF. Après avoir configuré un objet de chaîne de clés, vous pouvez l'utiliser pour définir l'authentification OSPFv2 pour une interface et pour une liaison virtuelle. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie. Pour savoir comment définir l'authentification pour une interface, consultez Configurer les paramètres d'interface OSPFv2, à la page 1057.

Pour configurer une chaîne de clés, procédez comme suit :

Procédure

Étape 1 Configurez une chaîne de clés avec un nom :

key chain*key-chain-name*

Exemple :

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)#
```

Vous pouvez maintenant définir les paramètres associés à la chaîne de clés.

Étape 2 Configurez l'identifiant de la chaîne de clés :

key*key-id*

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Exemple :

```
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)#
```

Étape 3 Configurez la clé ou le mot de passe de la chaîne de clés :

key-string [**0** | **8**] *key-string-text*

- Utilisez **0** pour indiquer qu'un mot de passe non chiffré suit, comme le montre l'exemple.
- Utilisez **8** pour indiquer qu'un mot de passe chiffré suit.
- La longueur maximale du mot de passe peut être de 80 caractères.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Exemple :

```
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)#
```

Étape 4 Configurez l'algorithme cryptographique pour la chaîne de clés :

cryptographic-algorithm*md5*

Vous devez fournir l'algorithme d'authentification cryptographique. Bien que la plateforme prenne en charge SHA1 et MD5, seul MD5 est pris en charge pour la gestion de la chaîne de clés.

Exemple :

```
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)#
```

Étape 5 (Facultatif) Configurez les paramètres de durée de vie de la chaîne de clés :

accept-lifetime [**local** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

send-lifetime [**ocal** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

Vous pouvez spécifier l'intervalle de temps nécessaire pour que le périphérique accepte ou envoie la clé lors de l'échange de clés avec un autre périphérique. L'heure de fin peut correspondre à la durée ou à l'heure absolue à laquelle la durée de vie de l'acceptation/envoi prend fin, ou être infinie.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie.

Exemple :

```
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite
ciscoasa(config-keychain-key)#
```

Vous pouvez utiliser la commande **show key chain** pour afficher la configuration de la chaîne de clés de démarrage sur le périphérique; **show run key chain** pour afficher la configuration de la chaîne de clés qui est actuellement en cours d'exécution sur le périphérique.

```
ciscoasa# show key chain
Key-chain CHAIN2:
    key 1 -- text "KEY1CHAIN2"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
  * key 2 -- text "(unset)"
        accept lifetime (11:00:12 UTC Sep 1 2018) - (11:12:12 UTC Sep 1 2018)
        send lifetime (always valid) - (always valid) [valid now]
Key-chain CHAIN1:
    key 1 -- text "CHAIN1KEY1STRING"
        accept lifetime (11:22:33 UTC Sep 1 2018) - (-1 seconds)
        send lifetime (always valid) - (always valid) [valid now]
ciscoasa#
```

```
ciscoasa# sh run key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# sh run key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

Prochaine étape

Vous pouvez maintenant appliquer la chaîne de clés configurée pour définir l'authentification OSPFv2 pour une interface.

- Configurer les paramètres d'interface OSPFv2, à la page 1057

Configurer le protocole OSPFv3

Cette section décrit les tâches nécessaires à la configuration d'un processus de routage OSPFv3.

Activer OSPFv3

Pour activer OSPFv3, vous devez créer un processus de routage OSPFv3, créer une zone pour OSPFv3, activer une interface pour OSPFv3, puis redistribuer la route dans les processus de routage OSPFv3 ciblés.

Procédure

Étape 1 Créez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# ipv6 router ospf 10
```

L'argument *process-id* est une balise utilisée en interne pour ce processus de routage et peut être n'importe quel entier positif. Cette balise ne doit pas nécessairement correspondre à la balise d'un autre appareil; elle est réservée à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Activez une interface :

interface *interface_name*

Exemple :

```
ciscoasa(config)# interface Gigabitethernet0/0
```

Étape 3 Créez le processus de routage OSPFv3 avec l'ID de processus spécifié et une zone pour le protocole OSPFv3 avec l'ID de zone spécifié :

ipv6 ospf *process-id* **area** *area_id*

Exemple :

```
ciscoasa(config)# ipv6 ospf 200 area 100
```

Configurer les paramètres d'interface OSPFv3

Vous pouvez modifier certains paramètres OSPFv3 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello et l'intervalle Dead. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 10
```

L'argument *process-id* est une balise utilisée en interne pour ce processus de routage et peut être n'importe quel entier positif. Cette balise ne doit pas nécessairement correspondre à la balise d'un autre appareil; elle est réservée à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Créez une zone OSPFv3 :

ipv6 ospf **area** [*area-num*] [**instance**]

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

L'argument *area-num* est la zone pour laquelle l'authentification doit être activée. Il peut s'agir d'une valeur décimale ou d'une adresse IP. Le mot clé **instance** spécifie l'ID d'instance de zone à attribuer à une interface. Une interface ne peut avoir qu'une seule zone OSPFv3. Vous pouvez utiliser la même zone sur plusieurs interfaces, et chaque interface peut utiliser un ID d'instance de zone différent.

Étape 3 Spécifiez le coût d'envoi d'un paquet sur une interface :

ipv6 ospf cost *interface-cost*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

L'argument *interface-cost* spécifie une valeur d'entier non signée exprimée sous forme de mesure d'état de liaison, dont la valeur peut aller de 1 à 65535. Le coût par défaut est basé sur la bande passante.

Étape 4 Filtrez les LSA sortants vers une interface OSPFv3 :

ipv6 ospf database-filter all out

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf database-filter all out
```

Tous les LSA sortants sont acheminés vers l'interface par défaut.

Étape 5 Définissez la durée en secondes pendant laquelle les paquets Hello ne doivent pas être vus avant que les voisins indiquent que le routeur est en panne :

ipv6 ospf dead-interval *seconds*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf dead-interval 60
```

La valeur doit être la même pour tous les nœuds du réseau et peut varier de 1 à 65 535. La valeur par défaut est quatre fois l'intervalle défini par la commande **ipv6 ospf hello-interval**.

Étape 6 Spécifiez le type de chiffrement d'une interface :

ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [[*key-encryption-type*] *key* | **null**}

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
```

```
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D
```

Le mot clé **ipsec** spécifie le protocole de sécurité IP. La paire mot clé-argument **spi** *spi* spécifie l'indice de la politique de sécurité, qui doit être compris entre 256 et 42949667295 et saisi sous forme décimale.

Le mot clé **esp** spécifie la charge utile de sécurité qui s'encapsule. L'argument *encryption-algorithm* spécifie l'algorithme de chiffrement à utiliser avec ESP. Les valeurs valides sont les suivantes :

- aes-cdc : active le chiffrement AES-CDC.
- 3des : active le chiffrement 3DES.
- des : active le chiffrement DES.
- null : spécifie ESP sans chiffrement.

L'argument *key-encryption-type* peut être l'une des deux valeurs suivantes :

- 0 : la clé n'est pas chiffrée.
- 7 : la clé est chiffrée.

L'argument *key* spécifie le nombre utilisé dans le calcul du condensé de message. Le nombre comporte 32 chiffres hexadécimaux (16 octets). La taille de la clé dépend de l'algorithme de chiffrement utilisé. Certains algorithmes, comme AES-CDC, vous permettent de choisir la taille de la clé. L'argument *authentication-algorithm* spécifie l'algorithme d'authentification de chiffrement à utiliser, qui peut être l'une des options suivantes :

- md5 : active le condensé de message 5 (MD5).
- sha1 : active SHA-1.

Le mot clé **null** remplace le chiffrement de zone.

Si le chiffrement OSPFv3 est activé sur une interface et qu'un voisin se trouve dans une zone différente (par exemple, la zone 0) et que vous souhaitez que l'ASA forme des contiguïtés avec cette zone, vous devez modifier la zone sur l'ASA. Après avoir modifié la zone sur l'ASA en 0, un délai de deux minutes est nécessaire avant que la contiguïté OSPFv3 ne se produise.

Étape 7 Spécifiez la réduction des inondations des LSA vers l'interface :

ipv6 ospf flood-reduction

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
```

```
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

Étape 8 Spécifiez l'intervalle en secondes entre les paquets Hello envoyés sur l'interface :

ipv6 ospf hello-interval *seconds*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf hello-interval 15
```

La valeur doit être la même pour tous les nœuds d'un réseau spécifique et peut varier de 1 à 65535. L'intervalle par défaut est de 10 secondes pour les interfaces Ethernet et de 30 secondes pour les interfaces de non-diffusion.

Étape 9 Ddésactivez la détection de la non-concordance MTU OSPF lors de la réception de paquets DBD :

ipv6 ospf mtu-ignore

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf mtu-ignore
```

La détection des incompatibilités MTU OSPF est activée par défaut.

Étape 10 Définissez le type de réseau OSPF sur un type autre que la valeur par défaut, qui dépend du type de réseau :

ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
```

```
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf network point-to-point non-broadcast
```

Le mot clé **point-to-point non-broadcast** définit le type de réseau sur point à point de non-diffusion. Le mot clé **broadcast** définit le type de réseau sur diffusion.

Étape 11 Définissez la priorité du routeur, qui aide à déterminer le routeur désigné pour un réseau :

ipv6 ospf priority *number-value*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf priority 4
```

Les valeurs valides sont comprises entre 0 et 255.

Étape 12 Configurez les interconnexions du routeur OSPFv3 avec les réseaux de non-diffusion :

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Étape 13 Spécifiez le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface :

ipv6 ospf retransmit-interval *seconds*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
```

```
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-interval 8
```

La durée doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

Étape 14 Définissez l'estimation du temps en secondes pour envoyer un paquet de mise à jour d'état de liaison sur l'interface.

ipv6 ospf transmit-delay *seconds*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-delay 3
```

Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 1 seconde.

Configurer les paramètres de routeur OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# ipv6 router ospf 10
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez les paramètres de zone OSPFv3 :

domaine

Exemple :

```
ciscoasa(config-rtr)# area 10
```

Les paramètres pris en charge comprennent l'ID de zone sous la forme d'une valeur décimale de 0 à 4294967295 et l'ID de zone dans le format d'adresse IP **A.B.C.D**.

Étape 3 Définissez une commande à sa valeur par défaut :

par défaut

Exemple :

```
ciscoasa(config-rtr)# default originate
```

Le paramètre **originate** distribue la route par défaut.

Étape 4 Contrôlez la distribution des renseignements par défaut :

default-information

Étape 5 Définissez la distance administrative de la route OSPFv3 en fonction du type de route :

distance

Exemple :

```
ciscoasa(config-rtr)# distance 200
```

Les paramètres pris en charge comprennent la distance administrative avec des valeurs de 1 à 254 et **ospf** pour la distance OSPFv3.

Étape 6 Supprimez l'envoi de messages de journal système avec le paramètre **lsa** lorsque le routeur reçoit une annonce d'état de liaison (LSA) pour les paquets OSPF de multidiffusion (MOSPF) de type 6 :

ignore

Exemple :

```
ciscoasa(config-rtr)# ignore lsa
```

Étape 7 Configurez le routeur pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est actif ou inactif :

log-adjacency-changes

Exemple :

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

Avec le paramètre **detail**, tous les changements d'état sont enregistrés.

Étape 8 Supprimez l'envoi et la réception des mises à jour de routage sur une interface :

passive-interface [*interface_name*]

Exemple :

```
ciscoasa(config-rtr)# passive-interface inside
```

L'argument *interface_name* spécifie le nom de l'interface sur laquelle le processus OSPFv3 est en cours d'exécution.

Étape 9 Configurez la redistribution des routes d'un domaine de routage vers un autre :

redistribute {**connected** | **ospf** | **static**}

Lieu :

- **connected** : spécifie les routes connectées.
- **ospf** : spécifie les routes OSPFv3.
- **static** : spécifie les routes statiques.

Exemple :

```
ciscoasa(config-rtr)# redistribute ospf
```

Étape 10 Créez un ID de routeur fixe pour un processus spécifié :

router-id {*A.B.C.D* | **cluster-pool** | **static**}

Lieu :

A.B.C.D : spécifie l'ID du routeur OSPF sous forme d'adresse IP.

cluster-pool : configure un ensemble d'adresses IP lorsque la mise en grappe d'interfaces individuelles est configurée. Pour en savoir plus sur les ensembles d'adresses IP utilisés dans la mise en grappe, consultez Configurer un ensemble d'adresses IP pour la mise en grappe (OSPFv2 et OSPFv3), à la page 1063.

Exemple :

```
ciscoasa(config-rtr)# router-id 10.1.1.1
```

Étape 11 Configurez les résumés d'adresses IPv6 avec des valeurs valides de 0 à 128 :

summary-prefix *X:X:X:X::X/*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 192.168.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

Le paramètre *X:X:X:X::X/* spécifie le préfixe IPv6.

Étape 12 Ajustez les minuteries de routage :

timers

Les paramètres des minuteries de routage sont les suivants :

- **lsa** : spécifie les minuteries LSA OSPFv3.
- **nsf** : spécifie les minuteries d'attente NSF OSPFv3.
- **pacing** : spécifie les minuteries de régulation OSPFv3.
- **throttle** : spécifie les minuteries de limitation OSPFv3.

Exemple :

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

Configurer les paramètres de zone OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535.

Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez le coût par défaut d'une zone NSSA ou d'une zone tampon :

area *area-id* **default-cost** *cost*

Exemple :

```
ciscoasa(config-rtr)# area 1 default-cost nssa
```

Étape 3 Résumez les routes qui correspondent à l'adresse et au masque pour les routeurs de frontière uniquement :

area *area-id* **range** *ipv6-prefix*/ *prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]

Exemple :

```
ciscoasa(config-rtr)# area 1 range FE01:1::1/64
```

- L'argument *area-id* identifie la zone pour laquelle les routes doivent être résumées. La valeur peut être spécifiée sous la forme d'une décimale ou d'un préfixe IPv6.

- L'argument *ipv6-prefix* spécifie le préfixe IPv6. L'argument *prefix-length* spécifie la longueur du préfixe.
- Le mot clé **advertise** définit l'état de la plage d'adresses à annoncer et génère un LSA récapitulatif de type 3.
- Le mot clé **not-advertise** définit l'état de la plage d'adresses sur DoNotAdvertise.
- Le LSA récapitulatif de type 3 est supprimé et les réseaux des composants restent masqués pour les autres réseaux.
- La paire mot clé-argument **cost** *cost* spécifie la mesure ou le coût de la route récapitulative, qui est utilisé lors des calculs de SPF OSPF pour déterminer les chemins les plus courts vers la destination.
- Les valeurs valides sont comprises entre 0 et 16 77 77 2015.

Étape 4 Précisez une zone NSSA :

area *area-id* **nssa**

Exemple :

```
ciscoasa(config-rtr)# area 1 nssa
```

Étape 5 Précisez une zone tampon :

area *area-id* **stub**

Exemple :

```
ciscoasa(config-rtr)# area 1 stub
```

Étape 6 Définissez un lien virtuel et ses paramètres :

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

Exemple :

```
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5
```

- L'argument *area-id* identifie la zone pour laquelle les routes doivent être résumées. Le mot clé **virtual link** spécifie la création d'un voisin de lien virtuel.
- L'argument *router-id* spécifie l'ID de routeur associé au voisin de lien virtuel.
- Saisissez la commande **show ospf** ou **show ipv6 ospf** pour afficher l'ID du routeur. Il n'y a pas de valeur par défaut.
- Le mot clé **hello-interval** spécifie le temps en secondes entre les paquets Hello qui sont envoyés sur une interface. L'intervalle Hello est un entier non signé qui doit être annoncé dans les paquets Hello. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 1 à 8 192. La valeur par défaut est 10.
- La paire mot clé-argument **retransmit-interval** *seconds* spécifie le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. L'intervalle de retransmission

est le délai aller-retour prévu entre deux routeurs du réseau associé. La valeur doit être supérieure au délai aller-retour attendu et peut varier de 1 à 8 192. La valeur par défaut est égale à 5.

- La paire mot clé-argument **transmit-delay** *seconds* spécifie le temps estimé en secondes nécessaire pour envoyer un paquet de mise à jour d'état de liaison sur l'interface. La valeur entière doit être supérieure à zéro. Les LSA dans le paquet de mise à jour ont leur propre âge incrémenté de cette quantité avant transmission. La plage de valeurs peut aller de 1 à 8 192. La valeur par défaut est 1.
- La paire mot clé-argument **dead-interval** *seconds* spécifie la durée en secondes pendant laquelle les paquets Hello ne sont pas vus avant qu'un voisin n'indique que le routeur est en panne. L'intervalle mort est un entier non signé. La valeur par défaut est quatre fois l'intervalle Hello, soit 40 secondes. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 1 à 8 192.
- Le mot clé **ttl-security hops** configure la sécurité de durée de vie (TTL) sur un lien virtuel. La valeur de l'argument *hop-count* peut aller de 1 à 254.

Configurer des interfaces passives OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process_id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Supprimez l'envoi et la réception des mises à jour de routage sur une interface :

passive-interface [*interface_name*]

Exemple :

```
ciscoasa(config-rtr)# passive-interface inside
```

L'argument *interface_name* spécifie le nom de l'interface sur laquelle le processus OSPFv3 est en cours d'exécution. Si l'argument *no interface_name* est spécifié, toutes les interfaces du processus OSPFv3 *process_id* sont rendues passives.

Configurer la distance administrative OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process_id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez la distance administrative pour les routes OSPFv3 :

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

Exemple :

```
ciscoasa(config-rtr)# distance ospf external 200
```

Le mot clé **ospf** spécifie les routes OSPFv3. Le mot clé **external** spécifie les routes externes de type 5 et de type 7 pour le protocole OSPFv3. Le mot clé **inter-area** spécifie les routes inter-zone pour le protocole OSPVv3. Le mot clé **intra-area** spécifie les routes intra-zone pour le protocole OSPFv3. L'argument *distance* spécifie la distance administrative, qui est un entier compris entre 10 et 254.

Configurer les minuteries mOSPFv3

Vous pouvez définir les minuteries d'arrivée des LSA, de cadence des LSA et de limitation pour le protocole OSPFv3.

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de

tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez l'intervalle minimum auquel l'ASA accepte les mêmes LSA de voisins OSPF :

timers lsa arrival *milliseconds*

Exemple :

```
ciscoasa(config-rtr)# timers lsa arrival 2000
```

L'argument *milliseconds* spécifie le délai minimum en millisecondes qui doit s'écouler entre l'acceptation de la même LSA provenant des voisins. La plage va de 0 à 6 000 000 millisecondes. La valeur par défaut est de 1 000 millisecondes.

Étape 3 Configurez la cadence des paquets LSA :

timers pacing flood *milliseconds*

Exemple :

```
ciscoasa(config-rtr)# timers lsa flood 20
```

L'argument *milliseconds* spécifie le temps en millisecondes auquel les LSA de la file d'attente de débordement sont cadencés entre les mises à jour. La plage configurable va de 5 à 100 millisecondes. La valeur par défaut est de 33 millisecondes.

Étape 4 Modifiez l'intervalle auquel les LSA OSPFv3 sont collectés dans un groupe et actualisés, additionnés ou rendus obsolètes :

timers pacing lsa-group *seconds*

Exemple :

```
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

L'argument *seconds* spécifie le nombre de secondes dans l'intervalle auquel les LSA sont regroupés, actualisés, additionnés ou rendus obsolètes. La plage va de 10 à 1 800 secondes. La valeur par défaut est 240secondes.

Étape 5 Configurez la cadence des paquets de retransmission LSA :

timers pacing retransmission *milliseconds*

Exemple :

```
ciscoasa(config-rtr)# timers pacing retransmission 100
```

L'argument *milliseconds* spécifie le temps en millisecondes auquel les LSA de la file d'attente de retransmission sont cadencés. La plage configurable va de 5 à 200 millisecondes. La valeur par défaut est de 66 millisecondes.

Étape 6 Configurez la limitation des LSA OSPFv3 :

timers throttle lsa *milliseconds1 milliseconds2 milliseconds3*

Exemple :

```
ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000
```

- L'argument *milliseconds1* spécifie le délai en millisecondes pour générer la première occurrence de LSA. L'argument *milliseconds2* spécifie le délai maximum en millisecondes pour générer le même LSA. L'argument *milliseconds3* spécifie le délai minimum en millisecondes pour générer le même LSA.
- Pour la limitation des LSA, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement cette valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.
- Pour *milliseconds1*, la valeur par défaut est 0 milliseconde.
- Pour *milliseconds2* et *milliseconds3*, la valeur par défaut est 5 000 millisecondes.

Étape 7 Configurez la limitation du SPF OSPFv3 :

timers throttle spf *milliseconds1 milliseconds2 milliseconds3*

Exemple :

```
ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000
```

- L'argument *milliseconds1* spécifie le délai en millisecondes avant de recevoir une modification du calcul SPF. L'argument *milliseconds2* spécifie le délai en millisecondes entre le premier et le deuxième calcul SPF. L'argument *milliseconds3* spécifie le temps d'attente maximum en millisecondes pour les calculs SPF.
- Pour la limitation SPF, si *milliseconds2* ou *milliseconds3* est inférieur à *milliseconds1*, le protocole OSPFv3 corrige automatiquement la valeur *milliseconds1*. De même, si *milliseconds3* est inférieur à *milliseconds2*, le protocole OSPFv3 corrige automatiquement la valeur *milliseconds2*.
- Pour *milliseconds1*, la valeur par défaut de la limitation SPF est de 5 000 millisecondes.
- Pour *milliseconds2* et *milliseconds3*, la valeur par défaut de la limitation SPF est de 10 000 millisecondes.

Définir les voisins OSPFv3 statiques

Vous devez définir des voisins OSPFv3 statiques pour annoncer les routes OSPF sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv3 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Avant de commencer, vous devez créer une route statique vers le voisin OSPFv3. Consultez Configurer une route statique, à la page 956 pour en savoir plus sur la création des routes statiques.

Procédure

Étape 1 Activez un processus de routage OSPFv3 et passez en mode de configuration du routeur IPv6.

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez les interconnexions du routeur OSPFv3 avec les réseaux de non-diffusion.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

Exemple :

```
ciscoasa(config-if)# interface ethernet0/0 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Réinitialiser les paramètres par défaut OSPFv3

Pour rétablir la valeur par défaut d'un paramètre OSPFv3, procédez comme suit :

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Renvoyez un paramètre facultatif à sa valeur par défaut :

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **discard-route | distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

Exemple :

```
ciscoasa(config-rtr)# default metric 5
```

- Le mot clé **area** spécifie les paramètres de zone OSPFv3. Le mot clé **auto-cost** spécifie le coût de l'interface OSPFv3 en fonction de la bande passante.
- Le mot clé **default-information** distribue les renseignements par défaut. Le mot clé **default-metric** spécifie la mesure d'une route redistribuée.
- Le mot clé **discard-route** active ou désactive l'installation d'une route rejetée. Le mot clé **distance** spécifie la distance administrative.
- Le mot clé **distribue-list** filtre les réseaux dans les mises à jour de routage.
- Le mot clé **ignore** ignore un événement particulier. Le mot clé **log-adjacency-changes** enregistre les modifications dans l'état de contiguïté.
- Le mot clé **maximum-paths** transfère les paquets sur plusieurs chemins.
- Le mot clé **passive-interface** supprime les mises à jour de routage sur une interface.
- Le mot clé **redistribute** redistribue les préfixes IPv6 à partir d'un autre protocole de routage.
- Le mot clé **router-id** spécifie l'ID de routeur pour le processus de routage indiqué.
- Le mot clé **summary-prefix** spécifie le préfixe récapitulatif IPv6.
- Le mot clé **timers** spécifie les minuteries du protocole OSPFv3.

Envoyer les messages du journal système

Configurez le routeur pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est actif ou inactif.

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez le routeur pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est actif ou inactif :

log-adjacency-changes [**detail**]

Exemple :

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

Le mot clé **detail** envoie un message de journal système pour chaque état, pas seulement lorsqu'un voisin OSPFv3 est activé ou désactivé.

Supprimer les messages du journal système

Pour supprimer l'envoi des messages de journal système lorsque la route reçoit des paquets LSA de type 6 OSPF multidiffusion (MOSPF) non pris en charge, procédez comme suit :

Procédure

Étape 1 Activez un processus de routage OSPFv2 :

router ospf *process_id*

Exemple :

```
ciscoasa(config-if)# router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Supprimez l'envoi des messages de journal système lorsque le routeur reçoit des paquets LSA de type 6 MOSPF non pris en charge :

ignore lsa mospf

Exemple :

```
ciscoasa(config-rtr)# ignore lsa mospf
```

Calculer les coûts récapitulatifs de la route

Procédure

Restaurez les méthodes utilisées pour calculer les coûts des routes récapitulatives conformément à la RFC 1583 :

compatible rfc1583

Exemple :

```
ciscoasa (config-rtr)# compatible rfc1583
```

Générer une route externe par défaut dans un domaine de routage OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Générez une route externe par défaut dans un domaine de routage OSPFv3 :

default-information originate [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*]

Exemple :

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
```

- Le mot clé **always** annonce la route par défaut, que cette dernière existe ou non.
- La paire mot clé-argument **metric** *metric-value* spécifie la mesure utilisée pour générer la route par défaut.
- Si vous ne spécifiez pas de valeur à l'aide de la commande **default-metric**, la valeur par défaut est 10. Les valeurs de mesure valides sont comprises entre 0 et 16777214.
- La paire mot clé-argment **metric-type** *type-value* spécifique le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides peuvent être l'une des valeurs suivantes :
  - 1. Route externe de type 1
  - 2. Route externe de type 2

  La valeur par défaut est la route externe de type 2.
- La paire mot clé-argument **route-map** *map-name* spécifie le processus de routage qui génère la route par défaut si la carte de routage est satisfaite.

Configurer un préfixe de résumé IPv6

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurer un préfixe de résumé IPv6 :

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# router-id 192.168.3.3
ciscoasa(config-rtr)# summary-prefix FECO::/24
ciscoasa(config-rtr)# redistribute static
```

L'argument *prefix* est le préfixe de routage IPv6 pour la destination. Le mot clé **not-advertise** supprime les routes qui correspondent à la paire préfixe-masque spécifiée. Ce mot clé s'applique uniquement à OSPFv3. La paire mot clé-argument **tag** *tag-value* spécifie la valeur de balise qui peut être utilisée comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage. Ce mot clé s'applique uniquement à OSPFv3.

Redistribuer les routes IPv6

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Redistribuez les routes IPv6 d'un processus OSPFv3 dans un autre :

redistribute *source-protocol* [*process-id*] [**include-connected** {[**level-1** | **level-2**}] [*as-number*] [**metric** [*metric-value* | **transparent**}] **[metric-type** *type-value*] [**match** {**external** [**1**|**2**] | **internal** | **nssa-external** [**1**|**2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

Exemple :

```
ciscoasa(config-rtr)# redistribute connected 5 type-1
```

- L'argument *source-protocol* spécifie le protocole source à partir duquel les routes sont redistribuées, qui peuvent être statiques, connectées ou OSPFv3.
- L'argument *process-id* est le numéro attribué administrativement lorsque le processus de routage OSPFv3 est activé.
- Le mot clé **include-connected** permet au protocole cible de redistribuer les routes apprises par le protocole source et les préfixes connectés sur les interfaces sur lesquelles le protocole source fonctionne.
- Le mot clé **level-1** indique que pour le protocole Intermediate System to Intermediate System (IS-IS), les routes de niveau 1 sont redistribuées dans d'autres protocoles de routage IP indépendamment.
- Le mot clé **level-1-2** indique que pour IS-IS, les routes de niveau 1 et de niveau 2 sont redistribuées dans d'autres protocoles de routage IP.
- Le mot clé **level-2** spécifie que pour IS-IS, les routes de niveau 2 sont redistribuées dans d'autres protocoles de routage IP indépendamment.
- Pour la paire mot clé-argument **metric** *metric-value*, lors de la redistribution d'un processus OSPFv3 dans un autre processus OSPFv3 sur le même routeur, la mesure est transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus vers un processus OSPFv3, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée.
- Le mot clé **metric transparent** permet au protocole RIP d'utiliser la mesure de la table de routage pour les routes redistribuées comme mesure RIP.
- La paire mot clé-argment **metric-type** *type-value* spécifique le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides peuvent être l'une des suivantes : 1 pour une route externe de type 1 ou 2 pour une route externe de type 2. Si aucune valeur n'est spécifiée pour le mot clé **metric-type**, l'ASA adopte une route externe de type 2. Pour IS-IS, le type de lien peut être de l'une des options suivantes : interne pour une mesure IS-IS inférieure à 63 ou externe pour une mesure IS-IS supérieure à 64 et inférieure à 128. La valeur par défaut est interne.
- Le mot clé **match** redistribue les routes dans d'autres domaines de routage et est utilisé avec l'une des options suivantes : **external** [**1**|**2**] (externe [1|2]) pour les routes externes au système autonome, mais qui sont importées dans le protocole OSPFv3 en tant que routes externes de type 1 ou de type 2; **internal** (interne) pour les routes internes à un système autonome donné; **nssa-external** [**1**|**2**] (nssa-externe [1|2]) pour les routes externes au système autonome, mais qui sont importées dans le protocole OSPFv3 dans une NSSA pour IPv6 en tant que routes externes de type 1 ou de type 2.

- La paire mots clé-argument **tag** *tag-value* spécifie la valeur décimale sur 32 bits associée à chaque route externe, qui peut être utilisée pour communiquer des informations entre ASBR. Si aucune valeur n'est spécifiée, le numéro du système autonome distant est utilisé pour les routages de BGP et EGP. Pour les autres protocoles, zéro est utilisé. Les valeurs valides vont de 0 à 4294967295.
- Le mot clé **route-map** spécifie la carte de routage à vérifier pour filtrer l'importation des routes du protocole de routage source au protocole de routage actuel. Si ce mot clé n'est pas spécifié, toutes les routes sont redistribuées. Si ce mot clé est spécifié, mais qu'aucune étiquette de carte de routage n'est répertoriée, aucune route n'est importée. L'argument *map-tag* identifie une carte de routage configurée.

Configurer le redémarrage progressif

L'ASA peut connaître des situations de défaillance connues qui ne devraient pas affecter le transfert de paquets sur la plateforme de commutation. La capacité de transfert sans arrêt (NSF) permet au transfert de données de se poursuivre le long des routes connues, pendant la restauration des informations du protocole de routage.

En mode de haute disponibilité, le processus OSPF redémarre lorsque l'unité active devient inactive et que l'unité en veille devient la nouvelle active. De même, en mode grappe, le processus OSPF redémarre lorsque l'unité de contrôle devient inactive et que l'unité de données est choisie comme nouvelle unité de contrôle. Ces processus de transition OSPF entraînent un retard considérable. Vous pouvez configurer NSF pour éviter la perte de trafic lors du changement d'état du processus OSPF. La fonctionnalité NSF est également utile lorsqu'une mise à niveau logicielle rapide est planifiée.

Le redémarrage progressif est pris en charge sur les protocoles OSPFv2 et OSPFv3. Vous pouvez configurer le redémarrage progressif sur OSPFv2 en utilisant NSF IETF (RFC 3623). Vous pouvez configurer le redémarrage progressif sur OSPFv3 à l'aide du redémarrage progressif (RFC 5187).

La configuration de la fonction de redémarrage progressif NSF comporte deux étapes : la configuration des capacités et la configuration d'un périphérique compatible avec NSF ou conscient de NSF. Un périphérique compatible NSF peut indiquer ses propres activités de redémarrage aux voisins, et il peut aider un voisin qui redémarre.

Un périphérique peut être configuré comme compatible NSF ou comme conscient de NSF, selon certaines conditions :

- Un périphérique peut être configuré comme compatible NSF, quel que soit le mode dans lequel il se trouve.
- Un périphérique doit être en mode de basculement ou de grappe EtherChannel étendu (L2) pour être configuré comme compatible NSF.
- Pour qu'un périphérique soit compatible NSF ou conscient de NSF, il doit être configuré de manière à traiter les blocs couvrant les publicités d'état de liaison (LSA) opaques et les signalisations locales de liaison (LLS), selon les besoins.

Remarque Lorsque des Hello rapides sont configurés pour le protocole OSPFv2, le redémarrage progressif ne se produit pas lorsque l'unité active est rechargée et que l'unité en veille devient active. En effet, le temps nécessaire au changement de rôle est supérieur à l'intervalle de temps mort configuré.

Configurer les capacités

Le mécanisme de redémarrage progressif de Cisco NSF dépend de la capacité de LLS, car il envoie un bloc LLS avec le bit RS défini dans le paquet Hello, pour indiquer l'activité de redémarrage. Le mécanisme IETF NSF dépend de la capacité de LSA opaque lorsqu'il envoie des LSA opaques de type 9 pour indiquer l'activité de redémarrage. Pour configurer les fonctionnalités, saisissez les commandes suivantes :

Procédure

Étape 1 Créez un processus de routage OSPF et entrez en mode de configuration de routeur pour le processus OSPF que vous souhaitez redistribuer :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument process_id est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Activez l'utilisation du bloc de données LLS ou de LSA opaques pour activer NSF :

capability {lls|opaque}

Le mot clé lls est utilisé pour activer la fonctionnalité LLS pour le mécanisme de redémarrage progressif de Cisco NSF.

Le mot clé opaque est utilisé pour activer la capacité de LSA opaque pour le mécanisme de redémarrage progressif IETF NSF.

Configuration du redémarrage progressif pour OSPFv2

Il existe deux mécanismes de redémarrage progressif pour OSPFv2, Cisco NSF et IETF NSF. Un seul de ces mécanismes de redémarrage progressif peut être configuré à la fois pour une instance ospf. Un périphérique conscient de NSF peut être configuré à la fois comme assistant NSF Cisco et comme assistant NSF IETF, mais un périphérique compatible avec NSF peut être configuré en mode Cisco NSF ou IETF NSF à la fois pour une instance ospf.

Configurer le redémarrage progressif de Cisco NSF pour OSPFv2

Configurez le redémarrage progressif de Cisco NSF pour OSPFv2, pour un périphérique compatible avec NSF ou conscient de NSF.

Procédure

Étape 1 Activez Cisco NSF sur un périphérique compatible avec NSF :

nsf cisco [enforce global]

Exemple :

```
ciscoasa(config-router)# nsf cisco
```

Le mot clé enforce global annule le redémarrage NSF lorsque des périphériques voisins non compatibles avec NSF sont détectés.

Étape 2 Activez le mode d'assistance de Cisco NSF sur le périphérique conscient de NSF :

capability {lls|opaque}

Exemple :

```
ciscoasa(config-router)# capability lls
```

Cette commande est activée par défaut. L'utilisation de la forme no (non) de la commande la désactive.

Configuration de la minuterie d'attente de redémarrage progressif pour le OSPF

Configurez le redémarrage progressif IETF NSF pour OSPFv2, pour un périphérique compatible avec NSF ou conscient de NSF.

Procédure

Étape 1 Activez IETF NSF sur un périphérique compatible avec NSF :

nsf ietf [restart-interval *seconds***]**

Exemple :

```
ciscoasa(config-router)# nsf ietf restart-interval 80
```

Vous pouvez spécifier la durée de l'intervalle de redémarrage progressif, en secondes. Les valeurs valides vont de 1 à 1 800 secondes. La valeur par défaut est 120secondes.

Le redémarrage progressif peut être interrompu si l'intervalle de redémarrage est configuré avec une valeur inférieure au temps nécessaire à la contiguïté. Par exemple, un intervalle de redémarrage inférieur à 30 secondes n'est pas pris en charge.

Étape 2 Activez le mode d'assistance IETF NSF sur le périphérique conscient de NSF :

nsf ietf helper [strict-lsa-checking]

Exemple :

```
ciscoasa(config-router)# nsf ietf helper
```

Le mot clé strict-LSA-checking indique que le routeur d'assistance mettra fin au processus de redémarrage du routeur s'il détecte une modification d'un LSA qui serait débordé vers le routeur qui redémarre, ou si un LSA modifié figure sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.

Cette commande est activée par défaut. L'utilisation de la forme no (non) de la commande la désactive.

Configuration du redémarrage progressif pour OSPFv3

La configuration de la fonctionnalité de redémarrage progressif NSF pour OSPFv3 comporte deux étapes : la configuration d'un périphérique pour qu'il soit compatible NSF, puis la configuration d'un périphérique pour qu'il soit conscient de NSF.

Procédure

Étape 1 Activez le traitement IPv6 sur une interface qui n'a pas été configurée avec une adresse IPv6 explicite :

interface physical_interface ipv6 enable

Exemple :

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

L'argument physical_interface identifie l'interface qui participe au protocole NSF OSPFv3.

Étape 2 Activez le redémarrage progressif pour le protocole OSPFv3 sur un appareil compatible NSF :

graceful-restart [restart interval seconds]

Exemple :

```
ciscoasa(config-router)# graceful-restart restart interval 80
```

L'intervalle de redémarrage en secondes spécifie la durée de l'intervalle de redémarrage progressif, en secondes. Les valeurs valides vont de 1 à 1 800 secondes. La valeur par défaut est 120secondes.

Le redémarrage progressif peut être interrompu si l'intervalle de redémarrage est configuré avec une valeur inférieure au temps nécessaire à la contiguïté. Par exemple, un intervalle de redémarrage inférieur à 30 secondes n'est pas pris en charge.

Étape 3 Activez le redémarrage progressif pour le protocole OSPFv3 sur un appareil conscient de NSF :

graceful-restart helper [strict-lsa-checking]

Exemple :

```
ciscoasa(config-router)# graceful-restart helper strict-lsa-checking
```

Le mot clé strict-LSA-checking indique que le routeur d'assistance mettra fin au processus de redémarrage du routeur s'il détecte une modification d'un LSA qui serait débordé vers le routeur qui redémarre, ou si un LSA modifié figure sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.

Le mode d'assistance du redémarrage progressif est activé par défaut.

Configuration de la minuterie d'attente de redémarrage progressif pour OSPF

On s'attend à ce que les routeurs OSPF définissent le bit RS dans l'EO-TLV associé à un paquet Hello lorsqu'on ne sait pas que tous les voisins sont répertoriés dans le paquet, mais que les routeurs qui redémarrent doivent conserver leurs contiguïtés. Cependant, la valeur du bit RS ne doit pas être supérieure aux secondes de RouterDeadInterval. Par conséquent, la commande **timers nsf wait** est introduite pour définir le bit RS dans les paquets Hello inférieurs aux secondes de RouterDeadInterval. La valeur par défaut de la minuterie d'attente de NSF est de 20 secondes.

Avant de commencer

- Pour configurer le délai d'attente de Cisco NSF pour OSPF, le périphérique doit être conscient de NSF ou compatible avec NSF.

Procédure

Étape 1 Entrez en mode de configuration du routeur OSPF.

Exemple :

```
ciscoasa(config)# router ospf
```

Étape 2 Entrez les minuteries et spécifiez nsf.

Exemple :

```
ciscoasa(config-router)# timers?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
```

Étape 3 Saisissez l'intervalle d'attente du redémarrage progressif. Cette valeur peut être comprise entre 1 et 65 535.

Exemple :

```
ciscoasa(config-router)# timers nsf wait 200
```

En utilisant l'intervalle d'attente du redémarrage progressif, vous pouvez vous assurer que l'intervalle d'attente n'est pas supérieur à l'intervalle de temps mort du routeur.

Supprimer la configuration OSPFv2

Supprimez la configuration OSPFv2.

Procédure

Supprimez toute la configuration OSPFv2 que vous avez activée.

clear configure router ospf *pid*

Exemple :

```
ciscoasa(config)# clear configure router ospf 1000
```

Une fois la configuration effacée, vous devez reconfigurer OSPF à l'aide de la commande **router ospf**.

Supprimer la configuration OSPFv3

Supprimez la configuration OSPFv3.

Procédure

Supprimez toute la configuration OSPFv3 que vous avez activée :

clear configure ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# clear configure ipv6 router ospf 1000
```

Une fois la configuration effacée, vous devez reconfigurer OSPFv3 à l'aide de la commande **ipv6 router ospf**.

Exemple de protocole OSPFv2

L'exemple suivant montre comment activer et configurer le protocole OSPFv2 avec différents processus facultatifs :

1. Pour activer le protocole OSPFv2, saisissez les commandes suivantes :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

2. (Facultatif) Pour redistribuer les routes d'un processus OSPFv2 vers un autre processus OSPFv2, saisissez les commandes suivantes :

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

3. (Facultatif) Pour configurer les paramètres d'interface OSPFv2, saisissez les commandes suivantes :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
ciscoasa(config-rtr)# interface inside
ciscoasa(config-interface)# ospf cost 20
ciscoasa(config-interface)# ospf retransmit-interval 15
ciscoasa(config-interface)# ospf transmit-delay 10
ciscoasa(config-interface)# ospf priority 20
ciscoasa(config-interface)# ospf hello-interval 10
ciscoasa(config-interface)# ospf dead-interval 40
ciscoasa(config-interface)# ospf authentication-key cisco
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
ciscoasa(config-interface)# ospf authentication message-digest
```

4. (Facultatif) Pour configurer les paramètres de zone OSPFv2, saisissez les commandes suivantes :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# area 0 authentication
ciscoasa(config-rtr)# area 0 authentication message-digest
ciscoasa(config-rtr)# area 17 stub
ciscoasa(config-rtr)# area 17 default-cost 20
```

5. (Facultatif) Pour configurer les minuteries de calcul de routage et afficher les messages de connexion et de déconnexion du voisinage, saisissez les commandes suivantes :

```
ciscoasa(config-rtr)# timers spf 10 120
ciscoasa(config-rtr)# log-adj-changes [detail]
```

6. (Facultatif) Pour afficher les paramètres de configuration OSPFv2 actuels, saisissez la commande **show ospf**.

   Voici un exemple de sortie de la commande **show ospf** :

```
ciscoasa(config)# show ospf

Routing Process "ospf 2" with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
```

```
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x 209a3
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

7. Pour effacer la configuration OSPFv2, utilisez la commande suivante :

```
ciscoasa(config)# clear configure router ospf pid
```

Exemples de protocole OSPFv3

L'exemple suivant montre comment activer et configurer le protocole OSPFv3 au niveau de l'interface :

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf 1 area 1
```

Voici un exemple de sortie de la commande **show running-config ipv6** :

```
ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
 log-adjacency-changes
```

Voici un exemple de sortie de la commande **show running-config interface** :

```
ciscoasa (config-if)# show running-config interface GigabitEthernet3/1
interface GigabitEthernet3/1
 nameif fda
 security-level 100
 ip address 1.1.11.1 255.255.255.0 standby 1.1.11.2
 ipv6 address 9098::10/64 standby 9098::11
 ipv6 enable
 ipv6 ospf 1 area 1
```

Les exemples suivants montrent comment configurer des interfaces spécifiques au protocole OSPFv3 :

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# nameif fda
ciscoasa (config-if)# security-level 100
ciscoasa (config-if)# ip address 10.1.11.1 255.255.255.0 standby 10.1.11.2
```

```
ciscoasa (config-if)# ipv6 address 9098::10/64 standby 9098::11
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf cost 900
ciscoasa (config-if)# ipv6 ospf hello-interval 20
ciscoasa (config-if)# ipv6 ospf network broadcast
ciscoasa (config-if)# ipv6 ospf database-filter all out
ciscoasa (config-if)# ipv6 ospf flood-reduction
ciscoasa (config-if)# ipv6 ospf mtu-ignore
ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
12345678901234567890123456789012

ciscoasa (config)# ipv6 router ospf 1
ciscoasa (config)# area 1 nssa
ciscoasa (config)# distance ospf intra-area 190 inter-area 100 external 100
ciscoasa (config)# timers lsa arrival 900
ciscoasa (config)# timers pacing flood 100
ciscoasa (config)# timers throttle lsa 900 900 900
ciscoasa (config)# passive-interface fda
ciscoasa (config)# log-adjacency-changes
ciscoasa (config)# redistribute connected metric 100 metric-type 1 tag 700
```

Pour un exemple de configuration d'une liaison virtuelle OSPFv3, consultez l'URL suivante :

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080b8fd06.shtml

Supervision OSPF

Vous pouvez afficher des statistiques spécifiques, comme le contenu des tables de routage IP, des caches et des bases de données. Vous pouvez également utiliser les renseignements fournis pour déterminer l'utilisation des ressources et résoudre les problèmes de réseau. Vous pouvez également afficher des renseignements sur l'accessibilité des nœuds et découvrir le chemin de routage emprunté par les paquets de votre périphérique à travers le réseau.

Pour superviser ou afficher diverses statistiques de routage OSPFv2, saisissez l'une des commandes suivantes :

Commande	Objectif
show ospf [*process-id* [*area-id*]]	Affiche des renseignements généraux sur les processus de routage OSPFv2.
show ospf border-routers	Affiche les entrées de la table de routage OSPFv2 interne vers l'ABR et l'ASBR.
show ospf [*process-id* [*area-id*]] database	Affiche des listes de renseignements concernant la base de données OSPFv2 pour un routeur en particulier.

Commande	Objectif
show ospf flood-list *if-name*	Affiche une liste des LSA en attente d'être inondés sur une interface (pour observer la cadence des paquets OSPFv2). Les paquets de mise à jour OSPFv2 sont automatiquement cadencés afin qu'ils ne soient pas envoyés à moins de 33 millisecondes d'intervalle. Sans cadence, certains paquets de mise à jour pourraient se perdre dans des situations où la liaison est lente, un voisin ne pourrait pas recevoir les mises à jour assez rapidement ou le routeur pourrait manquer d'espace tampon. Par exemple, sans cadence, des paquets pourraient être abandonnés si l'une des topologies suivantes existe : • Un routeur rapide est connecté à un routeur plus lent sur une liaison point à point. • Pendant l'inondation, plusieurs voisins envoient simultanément des mises à jour à un seul routeur. La cadence est également utilisée entre les renvois pour accroître l'efficacité et réduire au minimum les retransmissions perdues. Vous pouvez également afficher les LSA en attente d'envoi depuis une interface. La cadence permet d'envoyer plus efficacement les paquets de mise à jour et de retransmission OSPFv2. Il n'y a aucune tâche de configuration pour cette fonctionnalité; elle se produit automatiquement.
show ospf interface [*if_name*]	Affiche les renseignements sur l'interface liés au protocole OSPFv2.
show ospf neighbor [*interface-name*] [*neighbor-id*] [**detail**]	Affiche les renseignements sur le voisin OSPFv2 par interface.
show ospf request-list *neighbor if_name*	Affiche une liste de tous les LSA demandés par un routeur.
show ospf retransmission-list *neighbor if_name*	Affiche une liste de tous les LSA en attente de renvoi.
show ospf [*process-id*] summary-address	Affiche une liste de tous les renseignements de redistribution des adresses sommaires configurées dans le cadre d'un processus OSPFv2.
show ospf [*process-id*] **traffic**	Affiche une liste des différents types de paquets envoyés ou reçus par une instance OSPFv2 spécifique.
show ospf [*process-id*] virtual-links	Affiche les renseignements sur les liens virtuels liés au protocole OSPFv2.

Commande	Objectif
show route cluster	Affiche des renseignements supplémentaires sur la synchronisation des routes OSPFv2 dans la mise en grappe.

Pour superviser ou afficher diverses statistiques de routage OSPFv3, saisissez l'une des commandes suivantes :

Commande	Objectif
show ipv6 ospf [*process-id* [*area-id*]]	Affiche des renseignements généraux sur les processus de routage OSPFv3.
show ipv6 ospf [*process-id*] **border-routers**	Affiche les entrées de la table de routage OSPFv3 interne vers l'ABR et l'ASBR.
show ipv6 ospf [*process-id* [*area-id*]] database [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]	Affiche des listes de renseignements concernant la base de données OSPFv3 pour un routeur en particulier.
show ipv6 ospf [*process-id* [*area-id*]] **events**	Affiche les renseignements sur les événements OSPFv3.

Commande	Objectif
show ipv6 ospf [*process-id*] [*area-id*] flood-list *interface-type interface-number*	Affiche une liste des LSA en attente d'être inondés sur une interface (pour observer la cadence des paquets OSPFv3). Les paquets de mise à jour OSPFv3 sont automatiquement cadencés afin qu'ils ne soient pas envoyés à moins de 33 millisecondes d'intervalle. Sans cadence, certains paquets de mise à jour pourraient se perdre dans des situations où la liaison est lente, un voisin ne pourrait pas recevoir les mises à jour assez rapidement ou le routeur pourrait manquer d'espace tampon. Par exemple, sans cadence, des paquets pourraient être abandonnés si l'une des topologies suivantes existe : • Un routeur rapide est connecté à un routeur plus lent sur une liaison point à point. • Pendant l'inondation, plusieurs voisins envoient simultanément des mises à jour à un seul routeur. La cadence est également utilisée entre les retransmissions pour accroître l'efficacité et réduire au minimum les retransmissions perdues. Vous pouvez également afficher les LSA en attente d'envoi depuis une interface. La cadence permet d'envoyer plus efficacement les paquets de mise à jour et de retransmission OSPFv3. Il n'y a aucune tâche de configuration pour cette fonctionnalité; elle se produit automatiquement.
show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]	Affiche les renseignements sur l'interface liés au protocole OSPFv3.
show ipv6 ospf neighbor [*process-id*] [*area-id*] [*interface-type interface-number*] [*neighbor-id*] [**detail**]	Affiche les renseignements sur le voisin OSPFv3 par interface.
show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]	Affiche une liste de tous les LSA demandés par un routeur.
show ipv6 ospf [*process-id*] [*area-id*] retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]	Affiche une liste de tous les LSA en attente de renvoi.
show ipv6 ospf statistic [*process-id*] [**detail**]	Affiche diverses statistiques OSPFv3.
show ipv6 ospf [*process-id*] summary-prefix	Affiche une liste de tous les renseignements de redistribution des adresses sommaires configurées dans le cadre d'un processus OSPFv3.

Commande	Objectif
show ipv6 ospf [*process-id*] **timers** [**lsa-group** | **rate-limit**]	Affiche les renseignements sur les minuteries OSPFv3.
show ipv6 ospf [*process-id*] **traffic** [*interface_name*]	Affiche les statistiques relatives au trafic OSPFv3.
show ipv6 ospf virtual-links	Affiche les renseignements sur les liens virtuels liés au protocole OSPFv3.
show ipv6 route cluster [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]	Affiche le numéro de séquence de la table de routage IPv6, l'état de la minuterie de reconvergence IPv6 et le numéro de séquence des entrées de routage IPv6 dans une grappe.

Historique OSPF

Tableau 41 : Historique des fonctionnalités OSPF

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge OSPF	7.0(1)	Une prise en charge a été ajoutée pour les données de routage, l'authentification, la redistribution et la supervision des informations de routage à l'aide du protocole de routage Open Shortest Path First (OSPF). Nous avons introduit la commande suivante : **route ospf**
Routage dynamique en mode de contexte multiple	9.0(1)	Le routage OSPFv2 est pris en charge en mode de contexte multiple.
Mise en grappe	9.0(1)	Pour OSPFv2 et OSPFv3, la synchronisation groupée, la synchronisation du routage et l'équilibrage de charges EtherChannel étendu sont pris en charge dans l'environnement de mise en grappe. Nous avons introduit ou modifié les commandes suivantes : **show route cluster**, **show ipv6 route cluster**, **debug route cluster, router-id cluster-pool**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge OSPFv3 pour IPv6	9.0(1)	Le routage OSPFv3 est pris en charge pour IPv6. Nous avons introduit ou modifié les commandes suivantes : **ipv6 ospf**, **ipv6 ospf area**, **ipv6 ospf cost, ipv6 ospf database-filter all out, ipv6 ospf dead-interval, ipv6 ospf encryption, ipv6 ospf hello-interval, ipv6 ospf mtu-ignore, ipv6 ospf neighbor, ipv6 ospf network, ipv6 ospf flood-reduction, ipv6 ospf priority, ipv6 ospf retransmit-interval, ipv6 ospf transmit-delay, ipv6 router ospf, ipv6 router ospf area, ipv6 router ospf default, ipv6 router ospf default-information, ipv6 router ospf distance, ipv6 router ospf exit, ipv6 router ospf ignore, ipv6 router ospf log-adjacency-changes, ipv6 router ospf no, ipv6 router ospf passive-interface, ipv6 router ospf redistribute, ipv6 router ospf router-id, ipv6 router ospf summary-prefix, ipv6 router ospf timers, area encryption, area range, area stub, area nssa, area virtual-link, default, default-information originate, distance, ignore lsa mospf, log-adjacency-changes, redistribute, router-id, summary-prefix, timers lsa arrival, timers pacing flood, timers pacing lsa-group, timers pacing retransmission, timers throttle, show ipv6 ospf, show ipv6 ospf border-routers, show ipv6 ospf database, show ipv6 ospf events, show ipv6 ospf flood-list, show ipv6 ospf graceful-restart, show ipv6 ospf interface, show ipv6 ospf neighbor, show ipv6 ospf request-list, show ipv6 ospf retransmission-list, show ipv6 ospf statistic, show ipv6 ospf summary-prefix, show ipv6 ospf timers, show ipv6 ospf traffic, show ipv6 ospf virtual-links, show ospf, show running-config ipv6 router, clear ipv6 ospf, clear configure ipv6 router, debug ospfv3, ipv6 ospf neighbor**.
Prise en charge OSPF pour les Hellos rapides	9.2(1)	OSPF prend en charge la fonctionnalité Paquets Hello rapides, ce qui permet d'obtenir une configuration qui accélère la convergence dans un réseau OSPF. Nous avons modifié la commande suivante : **ospf dead-interval**
Minuteries	9.2(1)	De nouvelles minuteries OSPF ont été ajoutées; les anciennes ont été rendues obsolètes. Nous avons introduit les commandes suivantes : timers lsa arrival, timers pacing, timers throttle Nous avons supprimé les commandes suivantes : Timers spf, timers lsa-grouping-pacing
Filtrage des routes à l'aide de la liste d'accès	9.2(1)	Le filtrage des routes à l'aide d'ACL est désormais pris en charge. Nous avons introduit la commande suivante : distribute-list
Améliorations de la surveillance OSPF	9.2(1)	Des informations supplémentaires sur la surveillance OSPF ont été ajoutées. Nous avons modifié les commandes suivantes : show ospf events, show ospf rib, show ospf statistics, show ospf border-routers [detail], show ospf interface brief
OSPF redistribue le BGP	9.2(1)	La fonctionnalité de redistribution OSPF a été ajoutée. Nous avons ajouté la commande suivante : redistribute bgp

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge OSPF pour la transmission sans interruption (NSF)	9.3(1)	La prise en charge des protocoles OSPFv2 et OSPFv3 pour NSF a été ajoutée. Nous avons ajouté les commandes suivantes : capability, nsf cisco, nsf cisco helper, nsf ietf, nsf ietf helper, nsf ietf helper strict-lsa-checking, graceful-restart, graceful-restart helper, graceful-restart helper strict-lsa-checking
Prise en charge OSPF pour la transmission sans interruption (NSF)	9.13(1)	La minuterie d'attente NSF a été ajoutée. Nous avons ajouté une nouvelle commande pour définir la minuterie de l'intervalle de redémarrage NSF. Cette commande a été introduite pour s'assurer que l'intervalle d'attente n'est pas plus long que l'intervalle de temps mort du routeur. Nous avons introduit la commande suivante : **timers nsf wait <seconds>**



CHAPITRE 34

IS-IS

Ce chapitre décrit le protocole de routage IS-IS (Intermediate System to Intermediate System).

- À propos d'IS-IS, à la page 1105
- Conditions préalables d'IS-IS, à la page 1111
- Lignes directrices relatives à IS-IS, à la page 1112
- Configurer IS-IS, à la page 1112
- Supervision IS-IS, à la page 1143
- Historique d'IS-IS, à la page 1146
- Exemples d'IS-IS, à la page 1146

À propos d'IS-IS

Le protocole de routage IS-IS est un protocole IGP (Interior Gateway Protocol) à état de liaison. Les protocoles à état de liaison se caractérisent par la propagation des renseignements nécessaires pour créer une carte complète de la connectivité du réseau sur chaque périphérique participant. Cette carte est ensuite utilisée pour calculer le chemin le plus court vers les destinations. La mise en œuvre d'IS-IS prend en charge IPv4 et IPv6.

Vous pouvez diviser un domaine de routage en un ou plusieurs sous-domaines. Chaque sous-domaine est appelé une zone et se voit attribuer une adresse de zone. Le routage dans une zone est appelé routage de niveau 1. Le routage entre les zones de niveau 1 est appelé routage de niveau 2. Un routeur est appelé système intermédiaire (IS). Un IS peut fonctionner au niveau 1, au niveau 2 ou aux deux. Les IS qui fonctionnent au niveau 1 échangent des renseignements de routage avec d'autres IS de niveau 1 dans la même zone. Les IS qui fonctionnent au niveau 2 échangent des renseignements de routage avec d'autres routeurs de niveau 2, qu'ils se trouvent ou non dans la même zone de niveau 1. L'ensemble de routeurs de niveau 2 et les liaisons qui les relient forment le sous-domaine de niveau 2, qui ne doit pas être partitionné pour que le routage fonctionne correctement.

À propos de NET

Un IS est identifié par une adresse appelée Network Entity Title (NET). Le NET est l'adresse d'un point d'accès de service de réseau (NSAP), qui identifie une instance du protocole de routage IS-IS exécuté sur un IS. Le NET comporte de 8 à 20 octets et comprend les trois parties suivantes :

- Adresse de zone : ce champ a une longueur de 1 à 13 octets et est composé des octets de poids fort de l'adresse.

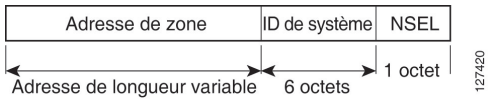
Remarque Vous pouvez attribuer plusieurs adresses de zone à une instance IS-IS; dans ce cas, toutes les adresses de zone sont considérées comme synonymes. Plusieurs adresses de zone synonymes sont utiles lors de la fusion ou de la division de zones dans le domaine. Une fois la fusion ou la division terminée, vous n'avez pas besoin d'attribuer plusieurs adresses de zone à une instance IS-IS.

- ID de système : ce champ a une longueur de 6 octets et suit immédiatement l'adresse de zone. Lorsque l'IS fonctionne au niveau 1, l'ID système doit être unique pour les périphériques de niveau 1 dans la même zone. Lorsque l'IS fonctionne au niveau 2, l'ID système doit être unique parmi tous les périphériques du domaine.

Remarque Vous attribuez un ID système à une instance IS.

- NSEL : le champ du sélecteur N a une longueur de 1 octet et suit immédiatement l'ID système. Il doit être défini sur 00.

Illustration 70 : Format NET



Nom de domaine dynamique IS-IS

Dans le domaine de routage IS-IS, l'ID système est utilisé pour représenter chaque ASA. L'ID système fait partie du NET configuré pour chaque ASA IS-IS. Par exemple, un ASA avec un NET configuré de 49.0001.0023.0003.000a.00 a un ID système de 0023.0003.000a. Le mappage du nom de l'ASA à l'ID système est difficile à mémoriser pour les administrateurs réseau lors de la maintenance et de la résolution des problèmes des ASA.

La saisie de la commande **show isis hostname** affiche les entrées du tableau de mappage de l'ID système au nom de l'ASA.

Le mécanisme de nom d'hôte dynamique utilise le protocole LSP (Link State Protocol) pour distribuer les renseignements de mappage du nom de l'ASA à l'D système sur l'ensemble du réseau. Chaque ASA du réseau tentera d'installer les renseignements de mappage de l'ID système au nom de l'ASA dans sa table de routage.

Si un ASA qui a annoncé le type de nom dynamique, la longueur et la valeur (TLV) sur le réseau cesse soudainement l'annonce, les derniers renseignements de mappage reçus resteront dans le tableau de mappage de l'hôte dynamique pendant une heure maximum, ce qui permettra à l'administrateur réseau d'afficher les entrées du tableau de mappage à un moment où le réseau rencontre des problèmes.

Types de PDU IS-IS

Les IS échangent des renseignements de routage avec leurs homologues à l'aide d'unités de données de protocole (PDU). Les types de PDU Hello Intermediate System-to-Intermediate System (IIH), de PDU d'état de liaison (LSP) et de PDU de numéro de séquence (SNP) sont utilisés.

IIH

Les IIH sont échangés entre les voisins IS sur les circuits sur lesquels le protocole IS-IS est activé. Les IIH comprennent l'ID système de l'expéditeur, la ou les adresses de zone attribuées et l'identité des voisins sur ce circuit connus de l'IS expéditeur. Des renseignements facultatifs supplémentaires peuvent également être inclus.

Il existe deux types d'IIH :

- IIH LAN de niveau 1 : ceux-ci sont envoyés sur les circuits multiaccès lorsque l'IS d'envoi fonctionne comme un appareil de niveau 1 sur ce circuit.
- IIH LAN de niveau 2 : ceux-ci sont envoyés sur les circuits multiaccès lorsque l'IS d'envoi fonctionne comme un appareil de niveau 2 sur ce circuit.

LSP

Un IS génère des LSP pour annoncer ses voisins et les destinations qui sont directement connectées à cet IS. Un LSP est identifié de façon unique par les éléments suivants :

- ID de système du IS qui a généré le LSP
- ID de pseudo-nœud : cette valeur est toujours égale à 0, sauf lorsque le LSP est un LSP de pseudo-nœud.
- Numéro LSP (0 à 255)
- Numéro de séquence de 32 bits

Chaque fois qu'une nouvelle version d'un LSP est générée, le numéro de séquence est incrémenté.

Les LSP de niveau 1 sont générés par les IS qui prennent en charge le niveau 1. Les LSP de niveau 1 sont inondés dans toute la zone de niveau 1. L'ensemble de LSP de niveau 1 généré par tous les IS de niveau 1 d'une zone constitue la base de données LSP de niveau 1 (LSPDB). Tous les IS de niveau 1 d'une zone ont une LSPDB de niveau 1 identique et, par conséquent, une carte de connectivité réseau identique pour la zone.

Les LSP de niveau 2 sont générés par les IS qui prennent en charge le niveau 2. Les LSP de niveau 2 sont inondés dans tout le sous-domaine de niveau 2. L'ensemble de LSP de niveau 2 généré par tous les IS de niveau 2 du domaine constitue la base de données LSP de niveau 2 (LSPDB). Tous les IS de niveau 2 ont une LSPDB de niveau 2 identique et, par conséquent, une carte de connectivité identique pour le sous-domaine de niveau 2.

SNP

Les SNP contiennent une description sommaire d'un ou de plusieurs LSP. Il existe deux types de SNP pour les niveaux 1 et 2 :

- Les PDU à numéro de séquence complet (CSNP) sont utilisées pour envoyer un résumé de la base de données LSPDB dont dispose un IS pour un niveau donné.
- Les PDU à numéro de séquence partiel (PSNP) sont utilisées pour envoyer un résumé d'un sous-ensemble des LSP pour un niveau donné qu'un IS possède dans sa base de données ou doit obtenir.

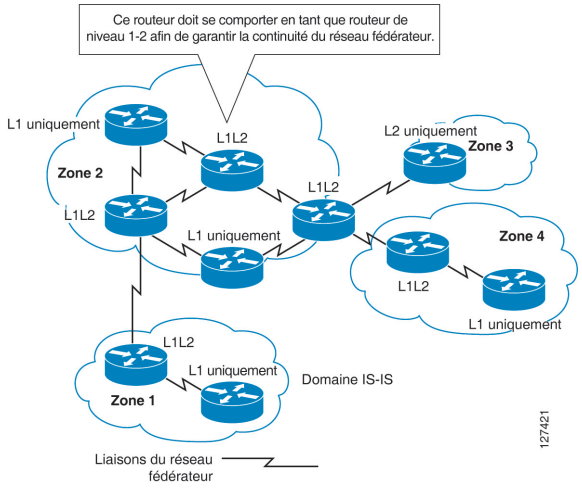
Fonctionnement d'IS-IS sur les circuits multiaccès

Les circuits multiaccès prennent en charge plusieurs IS, c'est-à-dire deux ou plus fonctionnant sur le circuit. Pour les circuits multiaccès, une condition préalable nécessaire est la capacité d'adresser plusieurs systèmes à l'aide d'une adresse de multidiffusion ou de diffusion. Un IS qui prend en charge le niveau 1 sur un circuit multiaccès envoie des IIH de niveau 1 LAN sur le circuit. Un IS qui prend en charge le niveau 2 sur un circuit multiaccès envoie des IIH LAN de niveau 2 sur le circuit. Les IS forment des contiguïtés distinctes pour chaque niveau avec les IS voisins sur le circuit.

Un IS forme une contiguïté de niveau 1 avec d'autres IS qui prennent en charge le niveau 1 sur le circuit et qui ont une adresse de zone correspondante. Deux ISE avec des ensembles dissociés d'adresses de zone prenant en charge le niveau 1 sur le même circuit multiaccès ne sont PAS pris en charge. Un IS forme une contiguïté de niveau 2 avec d'autres IS qui prennent en charge le niveau 2 sur le circuit.

Les périphériques de la topologie du réseau IS-IS dans la figure suivante effectuent le routage de niveau 1, de niveau 2 ou de niveau 1 et 2 le long du réseau fédérateur.

Illustration 71 : Périphériques de niveau 1, de niveau 2 et de niveau 1-2 dans une topologie de réseau IS-IS



Choix de l'IS désigné IS-IS

Si chaque IS annonce toutes ses contiguïtés sur un circuit de multiaccès dans ses LSP, le nombre total d'annonces requis serait de N 2 (où N est le nombre d'ISE qui fonctionnent à un niveau donné sur le circuit). Pour résoudre ce problème d'évolutivité, IS-IS définit un pseudo-nœud pour représenter le circuit de multiaccès. Tous les IS qui fonctionnent sur le circuit à un niveau donné choisissent un des IS pour qu'il agisse en tant que système intermédiaire désigné (DIS) sur ce circuit. Un DIS est choisi pour chaque niveau actif sur le circuit.

Le DIS est responsable de l'émission de LSP de pseudo-nœuds. Les LSP de pseudo-nœuds comprennent des annonces de voisins pour tous les IS qui fonctionnent sur ce circuit. Tous les IS qui fonctionnent sur le circuit (y compris le DIS) fournissent une annonce de voisin au pseudo-nœud dans leurs LSP non pseudo-nœuds et n'annoncent aucun de leurs voisins sur le circuit de multiaccès. De cette façon, le nombre total d'annonces requises varie en fonction du N, le nombre d'ISE qui fonctionnent sur le circuit.

Un LSP de pseudo-nœud est classifié de manière unique par les identifiants suivants :

- ID de système du DIS qui a généré le LSP

- Identifiant de pseudo-nœud (TOUJOURS NON ZÉRO)
- Numéro LSP (0 à 255)
- Numéro de séquence de 32 bits

L'ID de pseudo-nœud non zéro est ce qui différencie un LSP de pseudo-nœud d'un LSP non pseudo-nœud. Il est choisi par le DIS pour être unique parmi tous les autres circuits LAN pour lesquels il est également le DIS à ce niveau.

Le DIS est également responsable de l'envoi des CSNP périodiques sur le circuit. Cela fournit une description complète du contenu actuel de la LSPDB sur le DIS. D'autres IS sur le circuit peuvent alors effectuer les activités suivantes, ce qui synchronise de manière efficace et fiable les LSPDB de tous les IS sur un circuit multiaccès :

- Inonder les LSP qui sont absents de ou sont plus récents que ceux décrits dans les CSNP envoyés par le DIS.
- Demander un LSP en envoyant un PSNP pour les LSP décrits dans les CSNP envoyés par le DIS qui sont absents de la base de données locale ou plus anciens que ce qui est décrit dans l'ensemble CSNP.

Synchronisation LSPDB IS-IS

Le bon fonctionnement d'IS-IS nécessite un processus fiable et efficace pour synchroniser les LSPDB sur chaque IS. Dans IS-IS, ce processus s'appelle le processus de mise à jour. Le processus de mise à jour fonctionne indépendamment à chaque niveau pris en charge. Les LSP générés localement sont toujours de nouveaux LSP. Les LSP reçus d'un voisin sur un circuit peuvent être générés par un autre IS ou être une copie d'un LSP généré par l'IS local. Les LSP reçus peuvent être plus anciens, identiques ou plus récents que le contenu actuel de la LSPDB locale.

Traitement des nouveaux LSP

Lorsqu'un nouveau LSP est ajouté à la LSPDB locale, il remplace une ancienne copie du même LSP dans la LSPDB. Le nouveau LSP est marqué pour être envoyé sur tous les circuits sur lesquels l'IS a actuellement une contiguïté dans l'état UP au niveau associé au nouveau LSP, à l'exception du circuit sur lequel le nouveau LSP a été reçu.

Pour les circuits multiaccès, l'IS inonde une fois le nouveau LSP. L'IS examine l'ensemble des CNSP qui sont envoyés périodiquement par le DIS pour le circuit multiaccès. Si la LSPDB locale contient un ou plusieurs LSP plus récents que ceux décrits dans l'ensemble CSNP (y compris les LSP qui ne figurent pas dans l'ensemble CSNP), ces LSP sont rechargés sur le circuit multiaccès. Si la LSPDB locale contient un ou plusieurs LSP plus anciens que ceux décrits dans l'ensemble CSNP (y compris les LSP décrits dans l'ensemble CSNP qui sont absents de la LSPDB locale), un PSNP est envoyé sur le circuit multiaccès avec les descriptions des LSP qui nécessitent une mise à jour. Le DIS pour le circuit multiaccès répond en envoyant les LSP demandés.

Gestion des anciens LSP

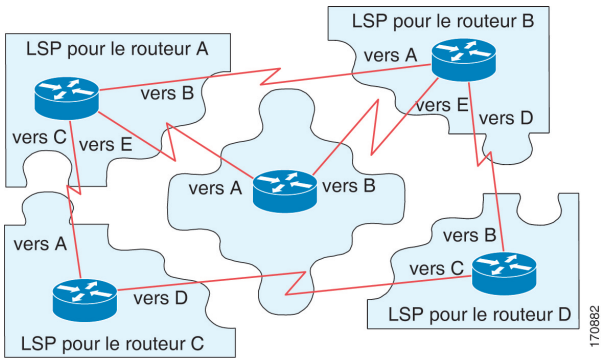
Un IS peut recevoir un LSP plus ancien que la copie dans la LSPDB locale. Un IS peut recevoir un SNP (complet ou partiel) qui décrit un LSP plus ancien que la copie dans la LSPDB locale. Dans les deux cas, l'IS marque le LSP dans la base de données locale à inonder sur le circuit sur lequel le LSP plus ancien ou le SNP contenant le LSP plus ancien a été reçu. Les actions entreprises sont les mêmes que celles décrites ci-dessus après l'ajout d'un nouveau LSP à la base de données locale.

Gestion des LSP du même âge

En raison de la nature distribuée du processus de mise à jour, il est possible qu'un IS reçoive des copies d'un LSP qui sont identiques au contenu actuel de la LSPDB locale. Dans les circuits multiaccès, la réception d'un LSP du même âge est ignorée. La transmission périodique d'un CSNP défini par le DIS pour ce circuit sert de confirmation implicite à l'expéditeur que le LSP a été reçu.

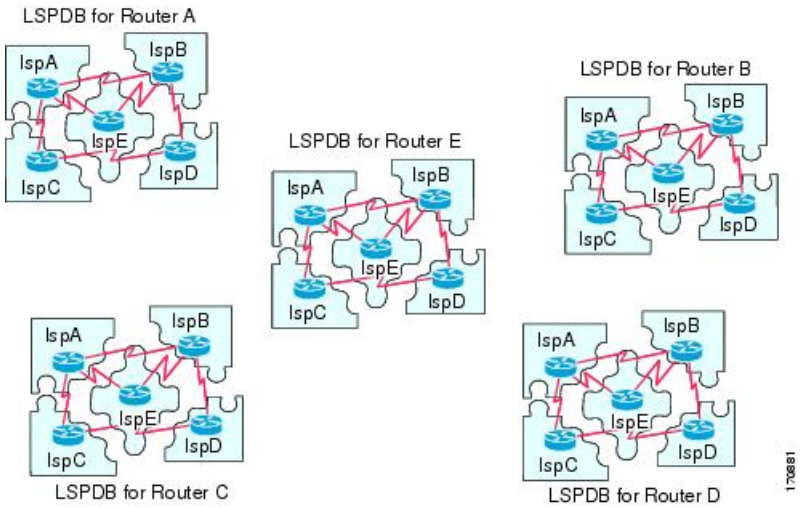
La figure suivante montre comment les LSP sont utilisés pour créer une carte du réseau. Considérez la topologie du réseau comme un casse-tête. Chaque LSP (représentant un IS) est l'une des pièces. Elle s'applique à tous les appareils de niveau 1 dans une zone ou à tous les appareils de niveau 2 dans un sous-domaine de niveau 2.

Illustration 72 : Carte du réseau IS-IS



La figure suivante montre chaque appareil du réseau IS-IS avec sa base de données d'état des liaisons entièrement mise à jour après la formation des contiguïtés entre les appareils voisins. Elle s'applique à tous les appareils de niveau 1 dans une zone ou à tous les appareils de niveau 2 dans un sous-domaine de niveau 2.

Illustration 73 : Périphériques IS-IS avec LSPDB synchronisées



Calcul du chemin le plus court IS-IS

Lorsque le contenu de la LSPDB change, chaque IS exécute indépendamment un calcul du chemin le plus court. L'algorithme est basé sur l'algorithme bien connu de Dijkstra pour trouver les chemins les plus courts le long d'un graphique orienté où les IS sont les sommets du graphe et les liaisons entre les IS sont des arêtes avec un poids non négatif. Une vérification de la connectivité bidirectionnelle est effectuée avant de prendre

en compte une liaison entre deux IS dans le graphique. Cela empêche l'utilisation de renseignements obsolètes dans la LSPDB, par exemple, lorsqu'un IS n'est plus opérationnel dans le réseau, mais n'a pas purgé l'ensemble de LSP qu'il a généré avant d'arrêter son fonctionnement.

La sortie du SPF est un ensemble de tuples (destination, prochain saut). Les destinations sont propres au protocole. Plusieurs chemins à coût égal sont pris en charge, auquel cas plusieurs sauts suivants seront associés à la même destination.

Des SPF indépendants sont effectués pour chaque niveau pris en charge par l'IS. Lorsque la même destination est accessible par les chemins de niveau 1 et 2, le chemin de niveau 1 est privilégié.

Un IS de niveau 2 qui indique qu'il a un ou plusieurs voisins de niveau 2 dans d'autres zones peut être utilisé par des périphériques de niveau 1 dans la même zone que le chemin de dernier recours, également appelé route par défaut. L'IS de niveau 2 indique sa liaison à d'autres zones en définissant un bit de connexion (ATT) dans son LSP de niveau 1 sur 0.



Remarque Un IS peut générer jusqu'à 256 LSP à chaque niveau. Les LSP sont identifiés par les numéros de 0 à 255. Le LSP 0 a des propriétés spéciales, notamment l'importance du réglage du bit ATT pour indiquer l'annexion à d'autres zones. Lorsque les LSP numérotés de 1 à 255 ont le bit ATT activé, ce n'est pas important.

Protocole d'arrêt IS-IS

Vous pouvez fermer IS-IS (le mettre dans un état administratif arrêté) pour apporter des modifications à la configuration du protocole IS-IS sans perdre vos paramètres de configuration. Vous pouvez fermer IS-IS au niveau du processus IS-IS global ou au niveau de l'interface. Si le périphérique a été redémarré lorsque le protocole a été désactivé, celui-ci devrait redémarrer dans un état désactivé. Lorsque le protocole est défini sur l'état administratif désactivé, les administrateurs réseau sont autorisés à désactiver administrativement le fonctionnement du protocole IS-IS sans perdre la configuration du protocole, à apporter une série de modifications à la configuration du protocole sans que le fonctionnement du protocole ne passe par des états intermédiaires, voire indésirables, puis à réactiver le protocole au moment opportun.

Conditions préalables d'IS-IS

Les conditions préalables suivantes sont nécessaires avant de configurer IS-IS :

- Connaissance des protocoles IPv4 et IPv6.
- Vous devez connaître la conception de votre réseau et la façon dont vous souhaitez que le trafic y passe avant de configurer IS-IS.
- Définissez les zones, préparez un plan d'adressage pour les périphériques (y compris la définition des réseaux) et déterminez les interfaces qui exécuteront IS-IS.
- Avant de configurer vos périphériques, préparez une matrice de contiguïtés qui indique les voisins attendus dans le tableau de contiguïté. Cela facilitera la vérification.

Lignes directrices relatives à IS-IS

Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Lignes directrices relatives à la grappe

Pris en charge uniquement en mode d'interface individuelle; le mode EtherChannel étendu n'est pas pris en charge.

Directives supplémentaires

IS-IS n'est pas pris en charge avec le transfert bidirectionnel.

Configurer IS-IS

Cette section décrit comment activer et configurer le processus IS-IS sur votre système.

Procédure

Étape 1 Activer le routage IS-IS globalement, à la page 1112.
Étape 2 Activer l'authentification IS-IS, à la page 1116.
Étape 3 Configurer LSP IS-IS, à la page 1120
Étape 4 Configurer les adresses de résumé IS-IS, à la page 1124.
Étape 5 Configurer les interfaces passives IS-IS, à la page 1125.
Étape 6 Configurer les interfaces IS-IS, à la page 1126.
Étape 7 Configurer le remplissage d'interfaces Hello IS-IS, à la page 1131
Étape 8 Configurer la famille d'adresses IPv4 IS-IS, à la page 1133.
Étape 9 Configurer la famille d'adresses IPv6 IS-IS, à la page 1138.

Activer le routage IS-IS globalement

La configuration IS-IS est effectuée en deux parties. Tout d'abord, vous configurez le processus IS-IS en mode de configuration globale, puis spécifiez le NET et le niveau de routage pour IS-IS en mode de configuration du routeur. D'autres paramètres généraux que vous pouvez configurer en mode de configuration du routeur peuvent avoir plus de sens pour votre réseau que de les configurer par interface. Cette section contient ces commandes.

Ensuite, vous activez le protocole IS-IS sur des interfaces individuelles en mode de configuration d'interface afin que l'interface participe au routage dynamique et forme des contiguïtés avec les appareils voisins. Vous devez activer le routage sur au moins une interface avant que des contiguïtés puissent être établies et que le

routage dynamique soit possible. Consultez Configurer les interfaces IS-IS, à la page 1126 pour connaître les procédures de configuration IS-IS sur les interfaces.

Cette procédure décrit comment activer IS-IS en tant que protocole de routage IP sur l'ASA et d'autres options générales en mode de configuration du routeur.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Activez IS-IS comme protocole de routage sur l'ASA :

router isis

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Étape 2 Spécifiez le NET pour le processus de routage :

net *network-entity-title*

Exemple :

```
ciscoasa(config-router)# net 49.1234.aaaa.bbbb.cccc.00
```

Le NET identifie le périphérique pour IS-IS. Consultez À propos de NET, à la page 1105 pour de plus amples renseignements sur le NET.

Étape 3 (Facultatif) Attribuez le niveau de routage pour le processus de routage IS-IS :

is-type [level-1 | level-2-only | level-1-2]

Exemple :

```
ciscoasa(config-router)# is-type level-1
```

- (Facultatif) **level-1** : indique le routage intra-zone. L'ASA apprend uniquement les destinations à l'intérieur de sa zone.
- (Facultatif) **level-2-only** : indique le routage inter-zone. L'ASA fait partie du réseau fédérateur et ne communique pas avec les routeurs de niveau 1 dans sa propre zone.
- (Facultatif) **level-1-2** : l'ASA effectue le routage de niveau 1 et de niveau 2. Ce routeur exécute deux instances du processus de routage. Il possède une LSDB pour les destinations à l'intérieur de la zone (routage de niveau 1) et exécute un calcul SPF pour découvrir la topologie de la zone. Il a également une autre LSDB avec les LSP de tous les autres routeurs du réseau fédérateur (niveau 2), et exécute un autre calcul SPF pour découvrir la topologie du réseau fédérateur et l'existence de toutes les autres zones.

Dans les configurations IS-IS traditionnelles, l'ASA agit à la fois comme un routeur de niveau 1 (intra-zone) et de niveau 2 (inter-zone). Dans les configurations IS-IS multizones, la première instance du processus de routage IS-IS configuré est par défaut un routeur de niveau 1-2 (intra-zone et inter-zone). Les autres instances du processus IS-IS configurées par défaut sont des routeurs de niveau 1.

Remarque
Nous vous conseillons fortement de configurer le type de processus de routage IS-IS.

Étape 4 Activez la fonctionnalité de nom d'hôte dynamique IS-IS sur l'ASA :

hostname dynamic

Cette commande est activée par défaut. Consultez Nom de domaine dynamique IS-IS, à la page 1106 pour obtenir des renseignements détaillés sur le nom d'hôte dynamique dans IS-IS.

Étape 5 Configurez le remplissage des messages Hello pour toutes les interfaces de l'ASA :

hello padding multi-point

Cette commande est activée par défaut. Elle configure les messages Hello IS-IS à la taille MTU complète. Cela permet une détection précoce des erreurs résultant de problèmes de transmission avec de grandes trames ou d'erreurs résultant de MTU non concordantes sur des interfaces adjacentes.

Vous pouvez désactiver le remplissage Hello (**no hello padding multi-point** pour toutes les interfaces sur un routeur pour le processus de routage IS-IS) pour éviter de gaspiller la bande passante du réseau dans le cas où la MTU des deux interfaces est identique ou en cas de pontage translationnel. Lorsque le remplissage Hello est désactivé, l'ASA envoie toujours les cinq premiers Hellos IS-IS remplis à la taille MTU complète afin de conserver les avantages de la détection des incompatibilités MTU.

Saisissez la commande **show clns interface** en mode d'exécution privilégié pour indiquer que le remplissage des messages Hello a été désactivé au niveau du routeur. Consultez Supervision IS-IS, à la page 1143 pour en savoir plus.

Étape 6 (Facultatif) Activez l'ASA pour générer un message de journal lorsqu'une contiguïté NLSP IS-IS change d'état (actif ou inactif) :

log-adjacency-changes [all]

Cette commande est désactivée par défaut. La journalisation des modifications de contiguïté est utile lors de la surveillance de grands réseaux. Les messages sont sous la forme suivante :

Exemple :

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

all : (Facultatif) Comprend les modifications générées par les événements non_IIH.

Étape 7 (Facultatif) Désactivez le protocole IS-IS afin qu'il ne puisse former aucune contiguïté sur aucune interface et effacez la base de données LSP :

protocol shutdown

Cette commande vous permet de désactiver le protocole IS-IS pour une instance de routage donnée, sans supprimer les paramètres de configuration IS-IS existants. Lorsque vous saisissez cette commande, le protocole IS-IS continue de s'exécuter sur le routeur et vous pouvez utiliser la configuration IS-IS actuelle, mais IS-IS ne forme aucune contiguïté sur aucune interface et efface également la base de données LSP IS-IS. Pour

désactiver IS-IS pour une interface en particulier, utilisez la commande **isis protocol shutdown**. Reportez-vous à Configurer les interfaces IS-IS, à la page 1126 pour connaître la procédure.

Étape 8 (Facultatif) Attribuez une priorité élevée à un préfixe IP IS-IS :

route priority high tag *tag-value*

Exemple :

```
ciscoasa(config-router)# route priority high tag 100
```

tag *tag-value* : affecte une priorité élevée à l'adresse IP IS-IS préfixée avec une balise de route spécifique. La plage va de 1 à 4294967295.

Utilisez cette commande pour baliser les préfixes IP IS-IS de priorité plus élevée pour un traitement et une installation plus rapides dans la table de routage globale, ce qui entraîne une convergence plus rapide. Par exemple, vous pouvez aider les adresses de passerelle VoIP à être traitées en premier pour que le trafic VoIP soit mis à jour plus rapidement que d'autres types de paquets.

Étape 9 (Facultatif) Modifiez globalement la valeur de la mesure pour toutes les interfaces IS-IS :

metric *default-value* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# metric 55 level-1
```

- *default-value* : la valeur de la mesure à attribuer au lien et à utiliser pour calculer le coût du chemin par les liaisons vers les destinations. La plage est de 1 à 63. La valeur par défaut est 10.
- (Facultatif) **level-1** : définit la mesure IPv4 ou IPv6 de niveau 1.
- (Facultatif) **level-2** : définit la mesure IPv4 ou IPv6 de niveau 2.

Nous vous conseillons d'utiliser la commande **metric** lorsque vous devez modifier la mesure par défaut pour toutes les interfaces IS-IS. Ceci évite les erreurs d'utilisateur, par exemple en supprimant involontairement une mesure définie d'une interface sans configurer de nouvelle valeur et en permettant à l'interface de revenir à la mesure par défaut de 10, devenant ainsi une interface privilégiée dans le réseau.

Étape 10 (Facultatif) Configurez l'ASA pour générer et accepter uniquement les nouveaux objets de longueur et de valeur (TLV) de nouveau type :

metric-style narrow | transition | wide [level-1 | level-2 | level-1-2]

Exemple :

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow** : utilise l'ancien type de TLV avec des mesures limitées.
- **transition** : demande à l'ASA d'accepter les anciens et les nouveaux types de TLV.
- **wide** : utilise le nouveau type de TLV pour transporter des mesures plus larges.
- (Facultatif) **level-1** : active cette commande sur le niveau de routage 1.
- (Facultatif) **level-2** : active cette commande sur le niveau de routage 2.

- (Facultatif) **level-1-2** : active cette commande sur les niveaux de routage 1 et 2.

Cette commande permet à l'ASA de générer et d'accepter uniquement de nouveaux TLV, ce qui fait que l'ASA utilise moins de mémoire et d'autres ressources que s'il génère à la fois des TLV d'ancien et de nouveau type.

Étape 11 (Facultatif) Configurez la priorité des ASA désignés sur toutes les interfaces :

priority *number-value*

Exemple :

```
ciscoasa(config-router)# priority 80
```

number-value : la priorité de l'ASA. La valeur doit être comprise entre 0 et 127. La valeur par défaut est 64.

Étape 12 (Facultatif) Configurez les adresses manuelles supplémentaires pour une zone IS-IS :

max-area-addresses *number*

Exemple :

```
ciscoasa(config-router)# max-area-addresses 3
```

number : le nombre d'adresses manuelles à ajouter. La plage se situe entre 3 et 254. Il n'y a pas de valeur par défaut.

Cette commande vous permet de maximiser la taille d'une zone IS-IS en configurant des adresses manuelles supplémentaires. Vous spécifiez le nombre d'adresses que vous souhaitez ajouter et attribuez une adresse NET pour créer chaque adresse manuelle. Consultez À propos de NET, à la page 1105 pour obtenir des renseignements sur le NET.

Étape 13 Configurez le partage de charge à chemins multiples pour IS-IS :

maximum-paths *number-of-paths*

Exemple :

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths : le nombre de routes à installer dans la table de routage. La plage va de 1 à 8. La valeur par défaut est 1.

La commande **maximum-path** est utilisée pour configurer le partage de charges multiples IS-IS lorsque ECMP est configuré dans l'ASA.

Activer l'authentification IS-IS

L'authentification du routage IS-IS empêche l'introduction de messages de routage non autorisés ou faux provenant de sources non approuvées. Vous pouvez définir un mot de passe pour chaque zone ou domaine IS-IS afin d'éviter que des routeurs non autorisés injectent de faux renseignements de routage dans la base de données sur l'état des liens, ou vous pouvez configurer un type d'authentification IS-IS, soit IS-IS MD5, soit une authentification en texte clair améliorée. Vous pouvez également définir l'authentification par interface.

Tous les voisins IS-IS sur les interfaces configurées pour l'authentification des messages IS-IS doivent être configurés avec le même mode d'authentification et la même clé pour que les contiguïtés soient établies.

Consultez À propos d'IS-IS, à la page 1105 pour en savoir plus sur les zones et les domaines.

Avant de commencer

Avant de pouvoir activer l'authentification du routage IS-IS, vous devez activer IS-IS et configurer une zone. Reportez-vous à Activer le routage IS-IS globalement, à la page 1112 pour connaître la procédure.

Procédure

Étape 1 Entrez en mode de configuration du routeur IS-IS et configurez un mot de passe d'authentification de zone IS-IS :

area-password *password* [**authenticate snp {validate | send-only}**]

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

- *password* : le mot de passe que vous attribuez.
- (Facultatif) **authenticate snp** : le système insère le mot de passe dans les SNP.
- **validate** : demande au système d'insérer le mot de passe dans les SNP et de vérifier le mot de passe dans les SNP qu'il reçoit.
- **send-only** : demande au système d'insérer uniquement le mot de passe dans les SNP, mais de ne pas vérifier le mot de passe dans les SNP qu'il reçoit. Utilisez ce mot clé lors d'une mise à niveau logicielle pour faciliter la transition.

L'utilisation de cette commande sur tous les ASA d'une zone empêche les routeurs non autorisés d'injecter de faux renseignements de routage dans la base de données sur l'état des liens. Cependant, ce mot de passe est échangé en texte brut et n'offre donc qu'une sécurité limitée.

Le mot de passe est inséré dans les LSP, CSNP et PSNP de niveau 1 (niveau du routeur de station). Si vous ne spécifiez pas le mot clé **authenticate snp** avec le mot clé **validate** ou **send-only**, le protocole IS-IS n'insère pas le mot de passe dans les SNP.

Étape 2 Entrez en mode de configuration du routeur IS-IS et configurez un mot de passe d'authentification de domaine IS-IS :

domain-password *password* [**authenticate snp {validate | send-only}**]

Exemple :

```
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

- *password* : le mot de passe que vous attribuez.
- (Facultatif) **authenticate snp** : permet au système d'insérer le mot de passe dans les unités PDU de numéro de séquence (SNP).

- **validate** : demande au système d'insérer le mot de passe dans les SNP et de vérifier le mot de passe dans les SNP qu'il reçoit.
- **send-only** : demande au système d'insérer uniquement le mot de passe dans les SNP, mais de ne pas vérifier le mot de passe dans les SNP qu'il reçoit. Utilisez ce mot clé lors d'une mise à niveau logicielle pour faciliter la transition.

Ce mot de passe est échangé en texte brut et n'offre donc qu'une sécurité limitée.

Le mot de passe est inséré dans les LSP, CSNP et PSNP de niveau 2 (niveau du routeur de zone). Si vous ne spécifiez pas le mot clé **authenticate snp** avec le mot clé **validate** ou **send-only**, le protocole IS-IS n'insère pas le mot de passe dans les SNP.

Étape 3 Configurez l'instance IS-IS globalement ou par interface pour que l'authentification soit effectuée uniquement sur les paquets IS-IS envoyés (non reçus) :

Mode de routeur :**authentication send-only [level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# authentication send-only level-1
```

Mode d'interface :**isis authentication send-only [level-1 | level-2]**

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis authentication send-only level-1
```

- (Facultatif) **level-1** : l'authentification n'est effectuée que sur les paquets de niveau 1 qui sont envoyés (non reçus).
- (Facultatif) **level-2** : l'authentification n'est effectuée que sur les paquets de niveau 2 qui sont envoyés (non reçus).

Utilisez cette commande avant de configurer le mode d'authentification et la chaîne de clés d'authentification afin que la mise en œuvre de l'authentification se déroule en douceur. Si vous ne spécifiez pas le niveau 1 ou le niveau 2, l'envoi s'applique uniquement aux deux niveaux.

Remarque
Les ASA auront plus de temps pour que les clés soient configurées sur chaque ASA si l'authentification est insérée uniquement dans les paquets en cours d'envoi, et n'est pas vérifiée sur les paquets en cours de réception. Une fois que tous les ASA qui doivent communiquer ont été configurés avec cette commande, activez le mode d'authentification et la chaîne de clés sur chaque ASA.

Étape 4 Précisez le type de mode d'authentification utilisé dans les paquets IS-IS pour l'instance IS-IS, globalement ou par interface :

Mode de routeur :**authentication mode {md5 | text} [level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# authentication mode md5 level-1
```

Mode d'interface :**isis authentication mode {md5 | text} [level-1 | level-2]**

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#  isis authentication mode md5 level-1
```

- **md5** : active l'authentification Message Digest 5.
- **text** : utilise l'authentification en texte clair.
- (Facultatif) **level-1** : active l'authentification spécifiée pour les paquets de niveau 1 uniquement.
- (Facultatif) **level-2** : active l'authentification spécifiée pour les paquets de niveau 2 uniquement.

Si vous avez configuré l'authentification en texte clair à l'aide de **area-password** ou **domain-password**, le mode d'authentification IS-IS remplace ces deux commandes. Si vous configurez **isis authentication mode** puis essayez de configurer **area-password** ou **domain-password**, vous n'êtes pas autorisé à le faire. Si vous ne spécifiez pas le niveau 1 ou le niveau 2, le mode s'applique uniquement aux deux niveaux.

Étape 5 Activez l'authentification pour IS-IS globalement ou par interface :

Mode de routeur : **authentication key [0 | 8]** *password* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Mode d'interface : **isis authentication key [0 | 8]** *password* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# router isis
ciscoasa(config-if)# isis authentication key 0 second level-1
```

- **0** : indique qu'un mot de passe non chiffré suivra.
- **8** : indique qu'un mot de passe chiffré suivra.
- *password* : active l'authentification et spécifie la clé.
- (Facultatif) **level-1** : active l'authentification pour les paquets de niveau 1 uniquement.
- (Facultatif) **level-2** : active l'authentification pour les paquets de niveau 2 uniquement.

Si aucun mot de passe n'est configuré avec la commande **key**, aucune authentification par clé n'est effectuée. L'authentification par clé peut s'appliquer à l'authentification en texte clair ou à l'authentification MD5. Reportez-vous à l'étape 4 pour définir le mode. Une seule clé d'authentification est appliquée à IS-IS à la fois. Si vous configurez une deuxième clé, la première est remplacée. Si vous ne spécifiez pas le niveau 1 ou le niveau 2, le mot de passe s'applique uniquement aux deux niveaux.

Étape 6 Configurez le mot de passe d'uthentification pour une interface :

isis password *password* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
```

```
ciscoasa(config-if)# isis password analyst level-1
```

- *password* : mot de passe d'authentification que vous attribuez à une interface.
- (Facultatif) **level-1** : configure le mot de passe d'authentification pour le niveau 1 de manière indépendante. Pour le routage de niveau 1, l'ASA agit en tant que routeur de station uniquement.
- (Facultatif) **level-2** : configure le mot de passe d'authentification pour le niveau 2 de manière indépendante. Pour le routage de niveau 2, l'ASA agit en tant que routeur de zone uniquement.

Cette commande vous permet d'empêcher des routeurs non autorisés de former des contiguïtés avec cet ASA et protège ainsi le réseau contre les intrusions. Le mot de passe est échangé en texte brut et offre ainsi une sécurité limitée. Vous pouvez attribuer différents mots de passe pour différents niveaux de routage en utilisant les mots clés **level-1** et **level-2**.

Exemples

L'exemple suivant montre une instance IS-IS avec l'authentification MD5 effectuée sur les paquets de niveau 1 et pour envoyer n'importe quelle clé appartenant à la chaîne de clés nommée site1 :

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Configurer LSP IS-IS

Un IS génère des LSP pour annoncer ses voisins et les destinations qui sont directement connectées à IS-IS. Consultez Types de PDU IS-IS, à la page 1106 pour en savoir plus sur les LSP.

Utilisez les commandes suivantes pour configurer les LSP afin d'avoir une configuration de convergence plus rapide.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Entrez en mode de configuration du routeur :

router isis

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Étape 2 Configurez l'ASA pour ignorer les LSP IS-IS qui sont reçus avec des erreurs de somme de contrôle interne plutôt que de purger les LSP :

ignore-lsp-errors

Exemple :

```
ciscoas(config-router)# ignore-lsp-errors
```

IS-IS exige qu'un LSP avec une somme de contrôle de liaison de données incorrecte soit purgé par le récepteur, ce qui oblige l'initiateur du paquet à le régénérer. Si un réseau a une liaison qui provoque la corruption de données tout en fournissant des LSP avec des sommes de contrôle de liaison de données correctes, un cycle continu de purge et de génération d'un grand nombre de paquets peut se produire, ce qui peut rendre le réseau non fonctionnel. Utilisez cette commande pour ignorer les LSP plutôt que de les purger. La valeur par défaut est Enabled (Activé).

Étape 3 Configurez IS-IS pour annoncer uniquement les préfixes appartenant aux interfaces passives :

advertise passive-only

Cette commande exclut les préfixes IP des réseaux connectés des annonces LSP et réduit ainsi le temps de convergence IS-IS, car moins de préfixes sont annoncés dans le LSP non pseudonode du routeur.

Étape 4 Configurez les LSP IS-IS pour qu'ils soient complets :

fast-flood *lsp-number*

Exemple :

```
ciscoasa(config-router)# fast-flood 7
```

(Facultatif) *lsp-number* : le nombre de LSP à inonder avant de lancer SPF.

Cette commande envoie un nombre spécifié de LSP à partir de l'ASA. Les LSP invoquent SPF avant d'exécuter SPF. L'accélération du processus d'inondation LSP améliore le temps de convergence global. La plage est comprise entre 1 et 15. La valeur par défaut est égale à 5.

Remarque
Nous vous conseillons d'activer l'inondation rapide des LSP avant que le routeur exécute le calcul SPF.

Étape 5 Configurez la taille MTU des LSP IS-IS :

lsp-mtu *bytes*

Exemple :

```
ciscoasa(config-router)# lsp-mtu 1300
```

bytes : taille maximale des paquet en octets. Le nombre d'octets doit être inférieur ou égal à la plus petite MTU de toute liaison du réseau. La plage se situe entre 128 et 4352.

Étape 6 Définissez la durée maximum pendant laquelle les LSP persistent dans la base de données de l'ASA sans être actualisés :

max-lsp-lifetime *seconds*

Exemple :

```
ciscoasa(config-router)# max-lsp-lifetime 2400
```

seconds : la durée de vie du LSP en secondes. La plage valide est de 1 à 65535. La valeur par défaut est 1200.

Si la durée de vie est dépassée avant qu'un LSP d'actualisation arrive, ce dernier est supprimé de la base de données.

Étape 7 Personnalisez la limitation IS-IS des calculs SPF :

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

Exemple :

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- (Facultatif) **level-1** : appliquer les intervalles aux zones de niveau 1 uniquement.
- (Facultatif) **level-2** : appliquer les intervalles aux zones de niveau 2 uniquement.
- *sf-max-wait* : indique l'intervalle maximal entre deux calculs SPF consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 10 secondes.
- (Facultatif) *sf-initial-wait* : indique le délai d'attente initial après une modification de topologie avant le premier calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente SPF maximum spécifié.
- (Facultatif) *spf-second-wait* : indique l'intervalle entre le premier et le deuxième calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

Les calculs SPF sont effectués uniquement lorsque la topologie change. Cette commande contrôle la fréquence à laquelle le logiciel effectue le calcul SPF.

Remarque
Le calcul SPF est exigeant pour le processeur. Par conséquent, il peut être utile de limiter la fréquence à laquelle il est effectué, en particulier lorsque la zone est vaste et que la topologie change souvent. L'augmentation de l'intervalle SPF réduit la charge du processeur de l'ASA, mais retarde potentiellement le taux de convergence.

Étape 8 Personnalisez la limitation IS-IS de la génération LSP :

lsp-gen-interval [level-1 | level-2] *lsp-max-wait [lsp-intial-wait lsp-second wait]*

Exemple :

```
ciscoasa(config-router)#  lsp-gen-interval level-1 2 50 100
```

- (Facultatif) **level-1** : appliquer les intervalles aux zones de niveau 1 uniquement.

- (Facultatif) **level-2** : appliquer les intervalles aux zones de niveau 2 uniquement.
- *lsp-max-wait* : indique l'intervalle maximum entre deux occurrences consécutives de génération d'un LSP. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- (Facultatif) *lsp-initial-wait* : indique le délai d'attente initial avant de générer le premier LSP. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 50 millisecondes.

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente LSP maximum spécifié.
- (Facultatif) *lsp-second-wait* : indique l'intervalle entre la première et la deuxième génération de LSP. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes (5 secondes).

  Cette commande contrôle le délai entre la génération des LSP.

Étape 9 Définissez l'intervalle d'actualisation du LSP :

lsp-refresh-interval *seconds*

Exemple :

```
ciscoasa(config-router)# lsp-refresh-interval 1080
```

(Facultatif) *seconds* : intervalle auquel les LSP sont actualisés. La plage valide est de 1 à 65 535 secondes. La valeur par défaut est 900 secondes (15 minutes).

L'intervalle d'actualisation détermine la vitesse à laquelle le logiciel transmet périodiquement dans les LSP les renseignements sur la topologie des routes qu'il génère. Il en est ainsi pour éviter que les renseignements de la base de données ne deviennent trop anciens.

Remarque
Les LSP doivent être actualisés périodiquement avant l'expiration de leur durée de vie. La valeur définie pour la commande **lsp-refresh-interval** doit être inférieure à la valeur définie pour la commande **max-lsp-lifetime**; sinon, les LSP expirent avant d'être actualisés. Si vous définissez une durée de vie des LSP trop faible par rapport à l'intervalle d'actualisation des LSP, le logiciel réduit l'intervalle d'actualisation des LSP pour empêcher les LSP d'expirer.

Étape 10 Personnalisez la limitation IS-IS des PRC :

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

Exemple :

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* : indique l'intervalle maximum entre deux calculs PRC consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- (Facultatif) *prc-initial-wait* : indique le délai d'attente initial du PRC après une modification de la topologie. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 2 000 millisecondes.

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente PRC maximum spécifié.
- (Facultatif) *prc-second-wait* : indique l'intervalle entre le premier et le deuxième calcul PRC. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes (5 secondes).

Le PRC est le processus logiciel de calcul des routes sans effectuer de calcul SPF. Cela est possible lorsque la topologie du système de routage lui-même n'a pas changé, mais qu'une modification est détectée dans les renseignements annoncés par un IS particulier ou lorsqu'il est nécessaire de tenter de réinstaller de telles routes dans la RIB.

Étape 11 Configurez les routes supprimées lorsque la PDU est pleine :

lsp-full suppress {external [interlevel] | interlevel [external] | none}

Exemple :

```
ciscoasa(config-router)# lsp-full suppress interlevel external
```

- **external** : supprime toutes les routes redistribuées sur cet ASA.
- **interlevel** : supprime toutes les routes provenant de l'autre niveau. Par exemple, si le LSP de niveau 2 est complet, les routes du niveau 1 sont supprimées.
- **none** : ne supprime aucune route.

Dans les réseaux où il n'y a aucune limite au nombre de routes redistribuées dans IS-IS (c'est-à-dire que la commande **redistribute maximum-prefix** n'est pas configurée), il est possible que le LSP soit saturé et que les routes soient supprimées. Utilisez la commande **lsp-full suppress** pour définir à l'avance quelles routes sont supprimées si le LSP est saturé.

Configurer les adresses de résumé IS-IS

Plusieurs groupes d'adresses peuvent être récapitulés pour un niveau donné. Les routes apprises d'autres protocoles de routage peuvent également être résumées. La métrique utilisée pour annoncer le résumé est la plus petite de toutes les routes spécifiques. Cela permet de réduire la taille de la table de routage.

Vous devez définir manuellement les adresses sommaires si vous souhaitez créer des adresses sommaires qui ne se produisent pas à la limite d'un numéro de réseau, ou si vous souhaitez utiliser des adresses sommaires sur l'ASA avec le récapitulatif de routage automatique désactivé.

Procédure

Étape 1 Entrez en mode de configuration du routeur :

router isis

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Étape 2 Créez des adresses agrégées pour IS-IS :

summary-address *address mask* **[level-1 | level-1-2 | level-2] tag** *tag-number* **metric** *metric-value*

Exemple :

```
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

- *address* : adresse sommaire désignée pour une plage d'adresses IP.
- *mask* – filtre d'adresse locale IP utilisé pour la route récapitulative.
- (Facultatif) **level-1** : seules les routes redistribuées au niveau 1 sont récapitulées avec l'adresse configurée et la valeur de masque.
- (Facultatif) **level-1-2** : les routes récapitulatives sont appliquées lors de la redistribution des routes de niveau 1 et niveau 2 et lorsque IS-IS de niveau 2 annonce des routes de niveau 1 comme accessibles dans sa zone.
- (Facultatif) **level-2** : les routes apprises par le routage de niveau 1 sont récapitulées dans le réseau fédérateur de niveau 2 avec l'adresse configurée et la valeur de masque. Les routes redistribuées dans IS-IS de niveau 2 sont également résumées.
- (Facultatif) **tag** *tag-number* : spécifie le numéro utilisé pour baliser la route récapitulative. La plage va de 1 à 4294967295.
- (Facultatif) **metric** *metric-value* : spécifie la valeur de la mesure appliquée à la route récapitulative. Le mot clé **metric** est attribué à la liaison et utilisé pour calculer le coût du chemin via les liaisons vers les destinations. Vous pouvez configurer cette mesure pour le routage de niveau 1 ou 2 uniquement. La plage va de 1 à 4294967295. La valeur par défaut est 10.

Saisissez la commande **show clns interface** pour vérifier les valeurs de mesure des interfaces. Consultez Supervision IS-IS, à la page 1143 pour en savoir plus.

Configurer les interfaces passives IS-IS

Vous pouvez désactiver les paquets Hello IS-IS et les mises à jour de routage sur les interfaces tout en incluant les adresses d'interface dans la base de données de topologie. Ces interfaces ne formeront pas de contiguïtés de voisins IS-IS.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage IS-IS, mais qui est associée à un réseau que vous souhaitez annoncer, configurez les interfaces passives (à l'aide de la commande **passive-interface**) pour empêcher cette interface d'utiliser IS-IS. En outre, vous pouvez spécifier la version d'IS-IS utilisée par l'ASA pour les mises à jour. Le routage passif aide à contrôler l'annonce des renseignements de routage IS-IS et désactive l'envoi et la réception des mises à jour de routage IS-IS sur une interface.

Procédure

Étape 1 Entrez en mode de configuration du routeur :

router isis

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Étape 2 Configurez une interface passive sur l'ASA :

passive-interface *interface-name*

Exemple :

```
ciscoasa(config-router)# passive-interface inside
```

- **default** : supprimez les mises à jour de routage sur toutes les interfaces.
- **management** : supprimez les mises à jour sur l'interface de gestion Management 0/1.
- **management2** : supprimez les mises à jour sur l'interface de gestion Management 0/2.
- **inside** : supprimez les mises à jour sur l'interface interne.

Cette commande configure les interfaces NON pas pour former des contiguïtés de voisins IS-IS, mais pour inclure les adresses d'interface dans la base de données IS-IS.

Étape 3 Configurez l'ASA pour annoncer les interfaces passives :

advertise passive-only

Exemple :

```
ciscoasa(config-router)# advertise passive-only
```

Cette commande configure IS-IS pour annoncer uniquement les préfixes qui appartiennent aux interfaces passives. Elle exclut les préfixes IP des réseaux connectés des annonces LSP, ce qui réduit le temps de convergence IS-IS.

Configurer les interfaces IS-IS

Cette procédure décrit comment modifier les interfaces ASA individuelles pour le routage IS-IS. Vous pouvez modifier les éléments suivants :

- Paramètres généraux tels que l'activation IS-IS, l'activation du protocole d'arrêt IS-IS, les priorités, les balises et les filtres de contiguïté sur une interface.
- Clé et mode d'authentification : consultez Activer l'authentification IS-IS, à la page 1116 pour connaître les procédures de configuration de l'authentification sur les interfaces.
- Valeurs de remplissage Hello : consultez Configurer le remplissage d'interfaces Hello IS-IS, à la page 1131 pour connaître les procédures de configuration du remplissage Hello sur les interfaces.
- Paramètres LSP
- La mesure du délai d'interface utilisée dans les calculs des mesures d'IS-IS.

Avant de commencer

Avant que le processus de routage IS-IS ne soit utile, vous devez attribuer un NET et certaines interfaces doivent avoir activé IS-IS. Vous ne pouvez configurer qu'un seul processus pour effectuer le routage de niveau 2 (inter-zone). Si le routage de niveau 2 est configuré sur un processus, tous les processus supplémentaires sont automatiquement configurés en tant que niveau 1. Vous pouvez configurer ce processus pour effectuer un routage intra-zone (niveau 1) en même temps. Une interface ne peut pas faire partie de plusieurs zones, sauf dans le cas où le processus de routage associé effectue à la fois le routage de niveau 1 et de niveau 2. Reportez-vous à Activer le routage IS-IS globalement, à la page 1112 pour connaître la procédure.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

Étape 2 Filtrez l'établissement des contiguïtés IS-IS :

isis adjacency-filter *nom* **[match-all]**

Exemple :

```
ciscoasa(config-if)# isis adjacency-filter ourfriends match-all
```

- *name* : nom de l'ensemble de filtres ou de l'expression à appliquer.
- (Facultatif) **match-all** : toutes les adresses NSAP doivent correspondre au filtre pour accepter la contiguïté. Si elle n'est pas spécifiée (par défaut), une seule adresse doit correspondre au filtre pour que la contiguïté soit acceptée.

Le filtrage est effectué en créant des adresses NSAP à partir des paquets Hello IS-IS entrants en combinant chaque adresse de zone du Hello avec l'ID de système. Chacune de ces adresses NSAP est ensuite transmise par le filtre. Si un NSAP correspond, le filtre est considéré comme transmis, sauf si le mot clé **match-all** est spécifié, auquel cas toutes les adresses doivent passer. La fonctionnalité du mot clé **match-all** est utile pour effectuer des tests négatifs, comme l'acceptation d'une contiguïté uniquement si une adresse particulière n'est pas présente.

Étape 3 Annoncez les préfixes IS-IS des réseaux connectés dans des annonces LSP sur une interface IS-IS :

isis advertise prefix

Exemple :

```
ciscoasa(config-if)# isis advertise prefix
```

Par défaut, cette commande est activée. Ainsi, les routes connectées sont distribuées même si elles ne sont pas destinées à être distribuées. Pour mettre fin à la redistribution inutile des routes connectées et améliorer

le temps de convergence IS-IS, utilisez la commande **no isis advertise prefix**. Cela exclut les préfixes IP du réseau connecté des annonces LSP et réduit le temps de convergence IS-IS.

Remarque
La configuration de la forme **no** de cette commande par interface IS-IS est une solution à petite échelle visant à réduire le temps de convergence IS-IS, car moins de préfixes sont annoncés dans le LSP non pseudo-nœud du routeur. Une alternative à la commande **isis advertise prefix** est la commande **advertise passive-only**, qui est une solution évolutive, car elle est configurée par instance IS-IS.

Étape 4 Activez IPv6 sur une interface IS-IS :

ipv6 router isis

Exemple :

```
ciscoasa(config-if)# ipv6 router isis
```

Étape 5 Configurez le délai entre les transmissions LSP IS-IS successives par interface :

isis lsp-interval *milliseconds*

Exemple :

```
ciscoasa(config-if)# isis lsp-interval 100
```

milliseconds : délai entre des LSP successifs. La plage se situe entre 1 et 4294967298. La valeur par défaut est de 33 millisecondes.

Dans les topologies avec un grand nombre de voisins et d'interfaces IS-IS, un ASA peut avoir de la difficulté avec la charge de CPU imposée par la transmission et la réception des LSP. Cette commande réduit le débit de transmission des LSP (et, par conséquent, le débit de réception des autres systèmes).

Étape 6 Configurez la valeur d'une mesure IS-IS :

isis metric {*metric-value* | **maximum**} [**level-1 | level-2**]

Exemple :

```
ciscoasa(config-if)# isis metric 15 level-1
```

- *metric-value* : mesure attribuée au lien et utilisée pour calculer le coût de chaque autre routeur par les liaisons du réseau vers d'autres destinations. Vous pouvez configurer cette mesure pour le routage de niveau 1 ou 2. La plage est comprise entre 1 et 63. La valeur par défaut est 10.
- **maximum** : exclut un lien ou une contiguïté dans le calcul SPF.
- (Facultatif) **level-1** : précise que cette mesure doit être utilisée uniquement dans le calcul SPF pour le routage de niveau 1 (intra-zone). Si aucun mot clé facultatif n'est spécifié, la mesure est activée sur les niveaux de routage 1 et 2.
- (Facultatif) **level-2** : précise que cette mesure doit être utilisée uniquement dans le calcul SPF pour le routage de niveau 2 (inter-zone). Si aucun mot clé facultatif n'est spécifié, la mesure est activée sur les niveaux de routage 1 et 2.

Étape 7 Configurez la priorité des ASA désignés sur l'interface :

isis priority *number-value* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-if)# isis priority 80 level-1
```

- *number-value* : définissez la priorité d'un ASA. La valeur doit être comprise entre 0 et 127. La valeur par défaut est 64.
- (Facultatif) **level-1** : définissez la priorité du niveau 1 indépendamment.
- (Facultatif) **level-2** : définissez la priorité du niveau 2 indépendamment.

La priorité est utilisée pour déterminer quel ASA d'un réseau local sera le routeur désigné ou le DIS. Les priorités sont annoncées dans les paquets Hello. L'ASA ayant la priorité la plus élevée devient le DIS.

Remarque
Dans IS-IS, il n'y a pas de routeur désigné de secours. La définition de la priorité à 0 réduit la probabilité que ce système devienne le DIS, mais ne l'empêche pas. Si un routeur ayant une priorité plus élevée entre en ligne, il prend le rôle du DIS actuel. En cas de priorités égales, l'adresse MAC la plus élevée rompt le lien.

Étape 8 Désactivez le protocole IS-IS afin qu'il ne puisse pas former de contiguïtés sur une interface spécifiée et placez l'adresse IP de l'interface dans le LSP généré par l'ASA :

isis protocol shutdown

Exemple :

```
ciscoasa(config-if)# isis protocol shutdown
```

Cette commande vous permet de désactiver le protocole IS-IS pour une interface spécifiée sans supprimer les paramètres de configuration. Le protocole IS-IS ne forme aucune contiguïté pour l'interface pour laquelle cette commande a été configurée, et l'adresse IP de l'interface est placée dans le LSP généré par le routeur. Utilisez la commande **protocol shutdown** si vous ne souhaitez pas que IS-IS forme une contiguïté sur n'importe quelle interface et efface la base de données LSP IS-IS. Reportez-vous à Activer le routage IS-IS globalement, à la page 1112 pour connaître la procédure.

Étape 9 Configurez le temps entre la retransmission de chaque LSP IS-IS :

isis retransmit-interval *seconds*

Exemple :

```
ciscoasa(config-if)#  isis retransmit-interval 60
```

(Facultatif) *seconds* : délai entre la retransmission de chaque LSP. Le nombre doit être supérieur au délai aller-retour attendu entre deux routeurs du réseau connecté. La valeur est comprise entre 0 et 65 535. La valeur par défaut est de 5 secondes.

Assurez-vous que l'argument *seconds* est prudent, sinon cela pourrait entraîner des retransmissions inutiles. Cette commande est sans effet sur les interfaces LAN (multipoint).

Étape 10 Configurez le temps entre les retransmissions de chaque LSP IS-IS :

isis retransmit-throttle-interval *milliseconds*

Exemple :

```
ciscoasa(config-if)#  isis retransmit-throttle-interval 300
```

(Facultatif) *milliseconds* : délai minimum entre les retransmissions des LSP sur l'interface. La valeur est comprise entre 0 et 65 535.

Cette commande peut être utile dans les très grands réseaux avec de nombreux LSP et de nombreuses interfaces comme moyen de contrôler le trafic de retransmission des LSP. Cette commande contrôle le débit auquel les LSP peuvent être renvoyés sur l'interface.

Cette commande est distincte du débit auquel les LSP sont envoyés sur l'interface (contrôlée par la commande **isis lsp-interval**) et de la période entre les retransmissions d'un seul LSP (contrôlée par la commande **isis retransmit-interval**). Vous pouvez utiliser ces commandes en combinaison pour contrôler la charge offerte de trafic de routage d'un ASA à ses voisins.

Étape 11 Définissez une balise sur l'adresse IP configurée pour une interface lorsque le préfixe IP est placé dans un LSP IS-IS :

isis tag *tag-number*

Exemple :

```
ciscoasa(config-if)# isis tag 100
```

tag-number : le numéro qui sert de balise sur une route IS-IS. La plage va de 1 à 4294967295.

Aucune action ne se produit sur une route balisée jusqu'à ce que la balise soit utilisée, par exemple, pour redistribuer ou synthétiser les routes. La configuration de cette commande déclenche l'ASA pour générer de nouveaux LSP, car la balise est une nouvelle information dans le paquet.

Exemples

Dans cet exemple, deux interfaces sont marquées avec des valeurs de balise différentes. Par défaut, ces deux adresses IP auraient été placées dans la base de données IS-IS de niveau 1 et de niveau 2. Cependant, si vous utilisez la commande **redistribute** avec une carte de routage pour faire correspondre la balise 110, seule l'adresse IP 172.16. 0.0 est placée dans la base de données de niveau 2.

```
ciscoasa (config)# interface GigabitEthernet1/0
ciscoasa (config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 120
ciscoasa (config)# interface GigabitEthernet1/1
ciscoasa (config-if)# ip address 172.16.0.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 110
ciscoasa (config-router)# route-map match-tag permit 10
ciscoasa (config-router)# match tag 110
ciscoasa (config)# router isis
ciscoasa (config-router)# net 49.0001.0001.0001.0001.00
ciscoasa (config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
```

Configurer le remplissage d'interfaces Hello IS-IS

Les paquets Hello sont responsables de la découverte et de la maintenance des voisins. Vous pouvez configurer les paramètres de remplissage Hello suivants au niveau de l'interface. Consultez Activer le routage IS-IS globalement, à la page 1112 pour activer/désactiver le remplissage Hello pour l'ensemble de l'IS-IS.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

Étape 2 Entrez dans le mode de configuration d'interface pour configurer le remplissage sur les unités de données de protocole Hello IS-IS (IIH PDU) pour toutes les interfaces de l'ASA :

isis hello padding

Exemple :

```
ciscoasa(config-if)# isis hello padding
```

Les messages Hello sont ajoutés à la MTU complète, ce qui permet une détection précoce des erreurs résultant de problèmes de transmission avec de grandes trames ou d'erreurs résultant de MTU non concordantes sur des interfaces adjacentes. Le remplissage Hello IS-IS est activé par défaut.

Remarque
Vous pouvez désactiver le remplissage Hello pour éviter de gaspiller la bande passante du réseau dans le cas où la MTU des deux interfaces est identique ou en cas de pontage translationnel. Bien que le remplissage Hello soit désactivé, les ASA envoient toujours les cinq premiers Hellos IS-IS remplis à la taille MTU complète afin de conserver les avantages de la détection des incompatibilités MTU.

Étape 3 Précisez la durée entre des paquets Hello consécutifs envoyés par IS-IS :

isis hello-interval {*seconds* | **minimal**} **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-if)# isis hello-interval 5 level-1
```

- *seconds* : la durée entre les paquets Hello. Par défaut, une valeur de trois fois les secondes d'intervalle Hello est annoncée comme délai de rétention dans les paquets Hello envoyés. Vous pouvez modifier le multiplicateur de 3 en configurant la commande **isis hello-multiplier**. Avec des intervalles Hello plus petits, les modifications topologiques sont détectées plus rapidement, mais le trafic de routage est plus élevé. La valeur est comprise entre 0 et 65 535. La valeur par défaut est 10.
- **minimal** : le système calcule l'intervalle Hello en fonction du multiplicateur Hello (spécifié par la commande **isis hello-multiplier**) de sorte que le délai de rétention résultant soit de 1 seconde.

- (Facultatif) **level-1** : configure l'intervalle Hello pour le niveau 1 indépendamment. Utilisez-le sur X.25, le service de données SMDS (Switched Multimegabit Data Service) et les réseaux multiaccès de relayage de trames.
- (Facultatif) **level-2** : configure l'intervalle Hello pour le niveau 2 indépendamment. Utilisez-le sur X.25, le SMDS et les réseaux multiaccès de relayage de trames.

Remarque
Bien qu'un intervalle Hello plus lent permette d'économiser de la bande passante et de réduire l'utilisation du processeur, il existe certaines situations où un intervalle Hello plus rapide est préférable, par exemple, une configuration de grande envergure qui utilise des tunnels d'ingénierie de trafic (TE). Si le tunnel TE utilise IS-IS comme protocole IGP (Interior Gateway Protocol) et que le processus de routage IP est redémarré au niveau du routeur au point d'entrée du réseau (tête), tous les tunnels TE sont resignalisés avec l'intervalle Hello par défaut. Un intervalle Hello plus rapide empêche cette nouvelle signalisation. Pour configurer un intervalle Hello plus rapide, vous devez augmenter l'intervalle Hello IS-IS manuellement à l'aide de la commande **isis hello-multiplier**.

Étape 4 Spécifiez le nombre de paquets Hello IS-IS qu'un voisin doit manquer avant que l'ASA déclare la contiguïté comme étant inactive :

isis hello-multiplier *multiplier* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-if)# isis hello-multiplier 10 level-1
```

- *multipler* : le délai de rétention annoncé dans les paquets Hello IS-IS est défini comme le produit du multiplicateur Hello par l'intervalle Hello. Les voisins déclarent une contiguïté à cet ASA après n'avoir reçu aucun paquet Hello IS-IS pendant le délai de rétention annoncé. Vous pouvez définir le délai de rétention (et donc le multiplicateur Hello et l'intervalle Hello) par interface, et il peut être différent entre les différents routeurs d'une même zone. La valeur doit être comprise entre 3 et 1 000. La valeur par défaut est de 3.
- (Facultatif) **level-1** : configure le multiplicateur Hello indépendamment pour les contiguïtés de niveau 1.
- (Facultatif) **level-2** : configure le multiplicateur Hello indépendamment pour les contiguïtés de niveau 2.

Utilisez cette commande dans les circonstances où les paquets Hello sont fréquemment perdus et que les contiguïtés IS-IS échouent inutilement.

Remarque
L'utilisation d'un multiplicateur Hello de petite taille entraînera une convergence rapide, mais peut entraîner une plus grande instabilité du routage. Modifiez le multiplicateur Hello à une valeur plus élevée pour contribuer à la stabilité du réseau, au besoin. Ne configurez jamais un multiplicateur Hello inférieur à la valeur par défaut de 3.

Étape 5 Configurez le type de contiguïté utilisé pour IS-IS :

isis circuit-type [level-1 | level-1-2 | level-2-only]

Exemple :

```
ciscoasa(config-if)# isis circuit-type level-2-only
```

- (Facultatif) **level-1** : configure un ASA pour la contiguïté de niveau 1 uniquement.
- (Facultatif) **level-1-2** : configure un ASA pour la contiguïté des niveaux 1 et 2.
- (Facultatif) **level-2** : configure un ASA pour la contiguïté de niveau 2 uniquement.

Vous n'avez normalement pas besoin de configurer cette commande. La méthode appropriée consiste à configurer le niveau sur un ASA. Reportez-vous à Activer le routage IS-IS globalement, à la page 1112 pour connaître la procédure. Vous devez configurer certaines interfaces comme niveau 2 uniquement sur les ASA situés entre les zones (routeurs de niveau 1-2). Cela permet d'économiser de la bande passante en envoyant des paquets Hello de niveau 1 inutilisés.

Étape 6 Configurez l'intervalle auquel les paquets CSNP périodiques sont envoyés sur les interfaces de diffusion :

isis csnp-interval *seconds* **[level-1 | level-1-2 | level-2]**

Exemple :

```
ciscoasa(config-if)#  isis csnp-interval 30 level-1
```

- *seconds* : intervalle entre la transmission des CSNP sur les réseaux multiaccès. Cet intervalle s'applique uniquement à l'ASA désigné. La valeur est comprise entre 0 et 65535. La valeur par défaut est de 10 secondes.
- (Facultatif) **level-1** : configure l'intervalle de temps entre la transmission des CSNP pour le niveau 1 indépendamment.
- (Facultatif) **level-2** : configure l'intervalle de temps entre la transmission des CSNP pour le niveau 2 indépendamment.

Il est peu probable que vous deviez modifier la valeur par défaut de cette commande.

Cette commande s'applique uniquement au DR pour une interface spécifiée. Seuls les DR envoient des paquets CSNP pour maintenir la synchronisation de la base de données. Vous pouvez configurer l'intervalle CSNP indépendamment pour les niveaux 1 et 2.

Configurer la famille d'adresses IPv4 IS-IS

Les routeurs sont autorisés à redistribuer des préfixes externes ou des routes apprises à partir de tout autre protocole de routage, configuration statique ou interface connectée. Les routes redistribuées sont autorisées dans un routeur de niveau 1 ou dans un routeur de niveau 2.

Vous pouvez configurer la contiguïté, Shortest Path First (SPF) et vous pouvez définir les conditions pour la redistribution des routes à partir d'un autre domaine de routage dans IS-IS (redistribution) pour les adresses IPv4.

Avant de commencer

Avant de pouvoir activer l'authentification du routage IS-IS, vous devez activer IS-IS et configurer une zone. Reportez-vous à Activer le routage IS-IS globalement, à la page 1112 pour connaître la procédure.

Procédure

Étape 1 Entrez en mode de configuration du routeur pour configurer une famille d'adresses IPv4 :

router isis

Exemple :

```
ciscoasa(config)# router isis
cisco(config-router)#
```

Étape 2 Effectuez une vérification de la contiguïté pour vérifier la prise en charge du protocole IS-IS :

adjacency-check

Exemple :

```
cisco(config-router)# adjacency-check
```

Étape 3 Définissez la distance administrative attribuée aux routes détectées par le protocole IS-IS :

distance *weight*

weight : distance administrative attribuée aux routes IS-IS. La plage va de 1 à 255. La valeur par défaut est 115.

Exemple :

```
ciscoasa(config-router)# distance 20
```

Cette commande configure les distances appliquées aux routes IS-IS lorsqu'elles sont insérées dans la RIB et influe sur la probabilité que ces routes soient préférées aux routes vers les mêmes adresses de destination découvertes par d'autres protocoles.

Remarque
En général, plus la valeur de la distance administrative est élevée, plus le taux de confiance est bas. Une distance administrative de 255 signifie que la source de renseignements de routage n'est pas du tout fiable et doit être ignorée. Les valeurs de poids sont subjectives; il n'existe aucune méthode quantitative pour choisir les valeurs de poids.

Étape 4 Configurez le partage de charge à chemins multiples pour IS-IS :

maximum-paths *number-of-paths*

Exemple :

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths : nombre de routes à installer dans la table de routage. La plage va de 1 à 8. La valeur par défaut est 1.

La commande **maximum-path** est utilisée pour configurer le partage de charges multiples IS-IS lorsque ECMP est configuré dans l'ASA.

Étape 5 Générez une route par défaut dans un domaine de routage IS-IS :

default-information originate [**route-map** *map-name*]

Exemple :

```
ciscoasa(config-router)# default-information originate route-map RMAP
```

(Facultatif) **route-map** *map-name* : le processus de routage génère la route par défaut si la carte de routage est satisfaite.

Si un ASA configuré avec cette commande a une route vers 0.0.0.0 dans la table de routage, IS-IS générera une annonce pour 0.0.0.0 dans ses LSP. Sans carte de routage, la valeur par défaut est annoncée uniquement dans les LSP de niveau 2. Pour le routage de niveau 1, il existe un autre mécanisme pour trouver la route par défaut, qui consiste à rechercher le routeur de niveau 1 ou 2 le plus proche. Le routeur de niveau 1 ou 2 le plus proche peut être trouvé en examinant l'ATT dans les LSP de niveau 1. Avec une commande **match ip address** *standard-access-list*, vous pouvez spécifier une ou plusieurs routes IP qui doivent exister avant que l'ASA annonce 0/0.

Étape 6 Définissez la mesure IS-IS globalement pour les niveaux 1 et 2 :

metric *default-value* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# metric 55 level-1
ciscoasa(config-router)# metric 45 level-2
```

- *default-value* : la valeur de la mesure à attribuer au lien et à utiliser pour calculer le coût du chemin par les liaisons vers les destinations. La plage est de 1 à 63. La valeur par défaut est 10.
- (Facultatif) **level-1** : définit la mesure IPv4 ou IPv6 de niveau 1.
- (Facultatif) **level-2** : définit la mesure IPv4 ou IPv6 de niveau 2.

Étape 7 Spécifiez le style de mesure et les niveaux auxquels l'appliquer :

metric-style [narrow | transition | wide] [level-1 | level-2 | level-1-2]

Exemple :

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow** : demande à l'ASA d'utiliser l'ancien type de TLV avec la mesure restrictive.
- **transition** : demande à l'ASA d'accepter les anciens et les nouveaux types TLV pendant la transition.
- **wide** : demande à l'ASA d'utiliser le nouveau type de TLV pour le transport de la mesure plus large.
- (Facultatif) **level-1** : définit la mesure IPv4 ou IPv6 de niveau 1.
- (Facultatif) **level-2** : définit la mesure IPv4 ou IPv6 de niveau 2.
- (Facultatif) **level-1-2** : définit la mesure IPv4 ou IPv6 des niveaux 1 et 2.

Étape 8 Spécifiez les contraintes concernant le moment où un routeur de niveau 1 au niveau 2 doit définir son bit associé :

set-attached-bit route-map *map-tag*

Exemple :

```
ciscoasa(config-router)# set-attached-bit route-map check-for-L2_backbone_connectivity
```

route-map *map-tag* : identifiant d'une carte de routage configurée. Si la carte de routage indiquée correspond, le routeur continue de définir son bit associé. Cette commande est désactivée par défaut.

Dans la mise en œuvre IS-IS actuelle, comme le spécifie la norme ISO 10589, les routeurs de niveau 1 et 2 définissent leur bit LSP associé de niveau 1 lorsqu'ils détectent d'autres zones dans leur propre domaine ou détectent d'autres domaines. Cependant, dans certaines topologies de réseau, les routeurs de niveau 1 au niveau 2 adjacents dans des zones différentes peuvent perdre la connectivité au réseau fédérateur de niveau 2. Les routeurs de niveau 1 peuvent ensuite envoyer le trafic destiné à l'extérieur de la zone ou du domaine aux routeurs de niveau 1 de niveau 2 qui peuvent ne pas avoir une telle connectivité.

Cette commande permet de mieux contrôler le paramètre de bit associé pour les routeurs de niveau 1 au niveau 2. La carte de routage peut spécifier une ou plusieurs routes CLNS. Si au moins une des clauses de correspondance des cartes de routage d'adresses de correspondance correspond à une route dans la table de routage CLNS de niveau 2 et si toutes les autres exigences de définition du bit associé sont respectées, le routeur de niveau 1 au niveau 2 continue de définir le bit associé dans son LSP de niveau 1. Si les exigences ne sont pas respectées ou si aucune clause de la carte de routage d'adresse de correspondance ne correspond à une route dans la table de routage CLNS de niveau 2, le bit associé n'est pas défini.

Étape 9 Configurez l'ASA pour signaler aux autres routeurs de ne pas l'utiliser comme saut intermédiaire dans leurs calculs SPF :

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

Exemple :

```
ciscoasa(config-router)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- (Facultatif) **on-startup** : définit le bit de surcharge au démarrage du système. Le bit de surcharge reste défini pendant le nombre de secondes configurées ou jusqu'à ce que le protocole BGP ait convergé, selon l'argument ou le mot clé ultérieur spécifié.
- (Facultatif) *seconds* : le nombre de secondes pendant lesquelles le bit de surcharge est défini au démarrage du système et reste défini. La plage va de 5 à 86 400.
- (Facultatif) **wait-for-bgp** : lorsque le mot clé **on-startup** est configuré, le bit de surcharge est défini au démarrage du système et reste défini jusqu'à ce que le protocole BGP ait convergé.
- (Facultatif) **suppress** : supprime le type de préfixe identifié par le ou les mots clés suivants.
- (Facultatif) **interlevel** : lorsque le mot clé **suppress** est configuré, empêche l'annonce des préfixes IP appris à partir d'un autre niveau IS-IS.
- (Facultatif) **external** : lorsque le mot clé **suppress** est configuré, empêche l'annonce des préfixes IP appris à partir d'autres protocoles.

Cette commande force l'ASA à définir le bit de surcharge (également connu sous le nom de bit hello) dans ses LSP non pseudo-nœuds. Normalement, le réglage du bit de surcharge est autorisé uniquement lorsqu'un ASA rencontre des problèmes. Par exemple, lorsqu'un ASA manque de mémoire, il se peut que la base de données de l'état des liaisons ne soit pas complète, ce qui entraîne une table de routage incomplète ou inexacte. En définissant le bit de surcharge dans ses LSP, les autres routeurs peuvent ignorer le routeur non fiable dans

leurs calculs SPF jusqu'à ce que le routeur ait résolu ses problèmes. Il en résulte qu'aucun chemin passant par ce routeur n'est visible par d'autres routes dans la zone IS-IS. Cependant, les préfixes IP et CLNS sont directement connectés à ce routeur.

Étape 10 Personnalisez la limitation IS-IS des PRC :

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

Exemple :

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* : indique l'intervalle maximum entre deux calculs PRC consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- (Facultatif) *prc-initial-wait* : indique le délai d'attente initial du PRC après une modification de la topologie. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 2 000 millisecondes.

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente PRC maximum spécifié.
- (Facultatif) *prc-second-wait* : indique l'intervalle entre le premier et le deuxième calcul PRC. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes (5 secondes).

  Le PRC est le processus logiciel de calcul des routes sans effectuer de calcul SPF. Cela est possible lorsque la topologie du système de routage lui-même n'a pas changé, mais qu'une modification est détectée dans les renseignements annoncés par un IS particulier ou lorsqu'il est nécessaire de tenter de réinstaller de telles routes dans la RIB.

Étape 11 Personnalisez la limitation IS-IS des calculs SPF :

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

Exemple :

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- (Facultatif) **level-1** : appliquer les intervalles aux zones de niveau 1 uniquement.
- (Facultatif) **level-2** : appliquer les intervalles aux zones de niveau 2 uniquement.
- *spf-max-wait* : indique l'intervalle maximum entre deux calculs SPF consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 10 secondes.
- (Facultatif) *spf-initial-wait* : indique le délai d'attente initial après une modification de topologie avant le premier calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente SPF maximum spécifié.
- (Facultatif) *spf-second-wait* : indique l'intervalle entre le premier et le deuxième calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

Les calculs SPF sont effectués uniquement lorsque la topologie change. Cette commande contrôle la fréquence à laquelle le logiciel effectue le calcul SPF.

Remarque
Le calcul SPF est exigeant pour le processeur. Par conséquent, il peut être utile de limiter la fréquence à laquelle il est effectué, en particulier lorsque la zone est vaste et que la topologie change souvent. L'augmentation de l'intervalle SPF réduit la charge du processeur de l'ASA, mais retarde potentiellement le taux de convergence.

Étape 12 Configurez IS-IS pour respecter les mesures externes lors des calculs SFP :

use external-metrics

Étape 13 Configurez une redistribution des routes BGP, connectées, IS-IS, OSPF ou statiques :

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

Exemple :

```
ciscoasa(config-router)# redistribute bgp level-1 metric-type internal metric 6
```

Remarque
La redistribution des routes statiques avec une carte de routage correspondant à une mesure n'est pas prise en charge.

metric *number* : valeur de la mesure. La plage va de 1 à 4294967295.

Configuration du bit associé

Dans l'exemple suivant, le bit associé restera défini lorsque le routeur correspondra à 49.00aa dans la table de routage L2 CLNS :

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

Configurer la famille d'adresses IPv6 IS-IS

Vous pouvez configurer la contiguïté, SPF et vous pouvez définir les conditions pour la redistribution des routes à partir d'un autre domaine de routage dans IS-IS (redistribution) pour les adresses IPv6.

Avant de commencer

Avant de pouvoir activer l'authentification du routage IS-IS, vous devez activer IS-IS et configurer une zone. Reportez-vous à Activer le routage IS-IS globalement, à la page 1112 pour connaître la procédure.

Procédure

Étape 1 Entrez en mode de configuration du routeur :

router isis

Exemple :

```
cisco(config-router)#
```

Étape 2 Spécifiez le style de mesure comme large :

metric-style wide [transition] [level-1 | level-2 | level-1-2]

Exemple :

```
ciscoas(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

- (Facultatif) **transition** : demande au routeur d'accepter les TLV de style ancien et nouveau.
- (Facultatif) **level-1** : définit la mesure IPv4 ou IPv6 de niveau 1.
- (Facultatif) **level-2** : définit la mesure IPv4 ou IPv6 de niveau 2.
- (Facultatif) **level-1-2** : définit la mesure IPv4 ou IPv6 des niveaux 1 et 2.

Nous vous conseillons d'utiliser la commande **metric** lorsque vous devez modifier la mesure par défaut pour toutes les interfaces IS-IS. Ceci évite les erreurs d'utilisateur, par exemple en supprimant involontairement une mesure définie d'une interface sans configurer de nouvelle valeur et en permettant à l'interface de revenir à la mesure par défaut de 10, devenant ainsi une interface privilégiée dans le réseau.

Étape 3 Passez en mode de configuration de famille d'adresses pour configurer les sessions de routage IS-IS qui utilisent des préfixes d'adresse IPv4 ou IPv6 standard :

address-family ipv6 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv6 unicast
cisco(config-router-af)#
```

Étape 4 Effectuez une vérification de la contiguïté pour vérifier la prise en charge du protocole IS-IS :

adjacency-check

Exemple :

```
cisco(config-router-af)# adjacency-check
```

Étape 5 Configurez le partage de charge à chemins multiples pour IS-IS :

maximum-paths *number-of-paths*

Exemple :

```
ciscoasa(config-router-af)# maximum-paths 8
```

number-of-paths : le nombre de routes à installer dans la table de routage. La plage va de 1 à 8. La valeur par défaut est 1.

La commande **maximum-path** est utilisée pour configurer le partage de charges multiples IS-IS lorsque ECMP est configuré dans l'ASA.

Étape 6 Définissez la distance administrative attribuée aux routes détectées par le protocole IS-IS :

distance *weight*

weight : la distance administrative attribuée aux routes IS-IS. La plage va de 1 à 255. La valeur par défaut est 115.

Exemple :

```
ciscoasa(config-router-af)# distance 20
```

Cette commande configure les distances appliquées aux routes IS-IS lorsqu'elles sont insérées dans la RIB et influe sur la probabilité que ces routes soient préférées aux routes vers les mêmes adresses de destination découvertes par d'autres protocoles.

Remarque
En général, plus la valeur de la distance administrative est élevée, plus le taux de confiance est bas. Une distance administrative de 255 signifie que la source de renseignements de routage n'est pas du tout fiable et doit être ignorée. Les valeurs de poids sont subjectives; il n'existe aucune méthode quantitative pour choisir les valeurs de poids.

Étape 7 Générez une route par défaut dans un domaine de routage IS-IS :

default-information originate [**route-map** *map-name*]

Exemple :

```
ciscoasa(config-router-af)# default-information originate route-map TEST7
```

(Facultatif) **route-map** *map-name* : le processus de routage génère la route par défaut si la carte de routage est satisfaite.

Si un ASA configuré avec cette commande a une route vers 0.0.0.0 dans la table de routage, IS-IS générera une annonce pour 0.0.0.0 dans ses LSP. Sans carte de routage, la valeur par défaut est annoncée uniquement dans les LSP de niveau 2. Pour le routage de niveau 1, il existe un autre mécanisme pour trouver la route par défaut, qui consiste à rechercher le routeur de niveau 1 ou 2 le plus proche. Le routeur de niveau 1 ou 2 le plus proche peut être trouvé en examinant l'ATT dans les LSP de niveau 1. Avec une commande **match ip address** *standard-access-list*, vous pouvez spécifier une ou plusieurs routes IP qui doivent exister avant que l'ASA annonce 0/0.

Étape 8 Configurez l'ASA pour signaler aux autres routeurs de ne pas l'utiliser comme saut intermédiaire dans leurs calculs SPF :

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

Exemple :

```
ciscoasa(config-router-af)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- (Facultatif) **on-startup** : définit le bit de surcharge au démarrage du système. Le bit de surcharge reste défini pendant le nombre de secondes configurées ou jusqu'à ce que le protocole BGP ait convergé, selon l'argument ou le mot clé ultérieur spécifié.
- (Facultatif) *seconds* : le nombre de secondes pendant lesquelles le bit de surcharge est défini au démarrage du système et reste défini. La plage va de 5 à 86 400.
- (Facultatif) **wait-for-bgp** : lorsque le mot clé **on-startup** est configuré, le bit de surcharge est défini au démarrage du système et reste défini jusqu'à ce que le protocole BGP ait convergé.
- (Facultatif) **suppress** : supprime le type de préfixe identifié par le ou les mots clés suivants.
- (Facultatif) **interlevel** : lorsque le mot clé **suppress** est configuré, empêche l'annonce des préfixes IP appris à partir d'un autre niveau IS-IS.
- (Facultatif) **external** : lorsque le mot clé **suppress** est configuré, empêche l'annonce des préfixes IP appris à partir d'autres protocoles.

Cette commande force l'ASA à définir le bit de surcharge (également connu sous le nom de bit hello) dans ses LSP non pseudo-nœuds. Normalement, le réglage du bit de surcharge est autorisé uniquement lorsqu'un ASA rencontre des problèmes. Par exemple, lorsqu'un ASA manque de mémoire, il se peut que la base de données de l'état des liaisons ne soit pas complète, ce qui entraîne une table de routage incomplète ou inexacte. En définissant le bit de surcharge dans ses LSP, les autres routeurs peuvent ignorer le routeur non fiable dans leurs calculs SPF jusqu'à ce que le routeur ait résolu ses problèmes. Il en résulte qu'aucun chemin passant par ce routeur n'est visible par d'autres routes dans la zone IS-IS. Cependant, les préfixes IP et CLNS sont directement connectés à ce routeur.

Étape 9 Personnalisez la limitation IS-IS des PRC :

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

Exemple :

```
ciscoasa(config-router-af)#  prc-interval 5 10 20
```

- *prc-max-wait* : indique l'intervalle maximum entre deux calculs PRC consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- (Facultatif) *prc-initial-wait* : indique le délai d'attente initial du PRC après une modification de la topologie. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 2 000 millisecondes.

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente PRC maximum spécifié.
- (Facultatif) *prc-second-wait* : indique l'intervalle entre le premier et le deuxième calcul PRC. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes (5 secondes).

  Le PRC est le processus logiciel de calcul des routes sans effectuer de calcul SPF. Cela est possible lorsque la topologie du système de routage lui-même n'a pas changé, mais qu'une modification est détectée dans les renseignements annoncés par un IS particulier ou lorsqu'il est nécessaire de tenter de réinstaller de telles routes dans la RIB.

Étape 10 Personnalisez la limitation IS-IS des calculs SPF :

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

Exemple :

```
ciscoasa(config-router-af)#  spf-interval level-1 5 10 20
```

- (Facultatif) **level-1** : appliquer les intervalles aux zones de niveau 1 uniquement.
- (Facultatif) **level-2** : appliquer les intervalles aux zones de niveau 2 uniquement.
- *spf-max-wait* : indique l'intervalle maximum entre deux calculs SPF consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 10 secondes.
- (Facultatif) *spf-initial-wait* : indique le délai d'attente initial après une modification de topologie avant le premier calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente SPF maximum spécifié.
- (Facultatif) *spf-second-wait* : indique l'intervalle entre le premier et le deuxième calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

Les calculs SPF sont effectués uniquement lorsque la topologie change. Cette commande contrôle la fréquence à laquelle le logiciel effectue le calcul SPF.

Remarque
Le calcul SPF est exigeant pour le processeur. Par conséquent, il peut être utile de limiter la fréquence à laquelle il est effectué, en particulier lorsque la zone est vaste et que la topologie change souvent. L'augmentation de l'intervalle SPF réduit la charge du processeur de l'ASA, mais retarde potentiellement le taux de convergence.

Étape 11 Configurez une redistribution des routes BGP, connectées, IS-IS, OSPF ou statiques :

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

Exemple :

```
ciscoasa(config-router-af)# redistribute static level-1 metric-type internal metric 6
```

metric *number*—The value for metric. La plage va de 1 à 4294967295.

Étape 12 Redistribuez les routes IS-IS uniquement du niveau 1 au niveau 2 ou du niveau 2 au niveau 1 :

redistribute isis {level-1 | level-2} into {level-2 | level-1} [[distribute-list *list-number* | **[route-map** *map-tag***]]**

Exemple :

```
ciscoasa(config-router-af)# redistribute isis level-1 into level-2
distribute-list 100
```

- **level-1 | level-2** : le niveau à partir duquel et vers lequel vous redistribuez les routes IS-IS.
- **into** : le mot clé qui sépare le niveau de routes redistribuées du niveau auquel vous redistribuez les routes.

- (Facultatif) **distribute-list** *list-number* : le numéro d'une liste de distribution qui contrôle la redistribution IS-IS. Vous pouvez spécifier une liste de distribution ou une carte de routage, mais pas les deux.
- (Facultatif) **route-map** *map-tag* : le nom d'une carte de routage qui contrôle la redistribution IS-IS. Vous pouvez spécifier une liste de distribution ou une carte de routage, mais pas les deux.

Remarque
Vous devez spécifier la commande **metric-style wide** pour que la commande **redistribute isis** fonctionne. Reportez-vous à l'étape 1 de cette procédure.

Dans IS-IS, toutes les zones sont des zones tampons, ce qui signifie qu'aucun renseignement de routage ne fuite du réseau fédérateur (niveau 2) vers les zones (niveau 1). Les routeurs de niveau 1 uniquement utilisent le routage par défaut vers le routeur de niveau 1-niveau 2 le plus proche dans leur zone. Cette commande vous permet de redistribuer les routes IP de niveau 2 dans les zones de niveau 1. Cette redistribution permet aux routeurs de niveau 1 uniquement de choisir le meilleur chemin pour qu'un préfixe IP sorte de la zone. Il s'agit d'une fonctionnalité IP uniquement, le routage CLNS est toujours un routage stub.

Remarque
Pour plus de contrôle et de stabilité, vous pouvez configurer une liste de distribution ou une carte de routage afin de contrôler les routes IP de niveau 2 pouvant être redistribuées dans le niveau 1. Cela permet aux grands réseaux IS-IS-IP d'utiliser la zone pour une meilleure évolutivité.

Étape 13 Créez des préfixes agrégés pour les routes IS-IS IPv6 :

summary-prefix *ipv6-prefix* **[level-1 | level-1-2 | level-2]**

Exemple :

```
cisco(config-router-af)# summary-prefix 2001::/96 level-1
```

- *ipv6 address* : le préfixe IPv6 sous la forme X.X.X.X.::X/0-128.
- (Facultatif) **level-1** : seules les routes redistribuées au niveau 1 sont récapitulées avec l'adresse configurée et la valeur de masque.
- (Facultatif) **level-1-2** : les routes récapitulatives sont appliquées lors de la redistribution des routes dans IS-IS de niveau 1 et niveau 2 et lorsque IS-IS de niveau 2 annonce des routes de niveau 1 comme accessibles dans sa zone.
- (Facultatif) **level-2** : les routes apprises par le routage de niveau 1 sont récapitulées dans le réseau fédérateur de niveau 2 avec l'adresse configurée et la valeur de masque. Les routes redistribuées dans IS-IS de niveau 2 sont également résumées.

Supervision IS-IS

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage IS-IS. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande.

Supervision de la base de données IS-IS

Utilisez les commandes suivantes pour superviser la base de données IS-IS :

- **show isis database [level-1 | l1] [level-2 | l2] [detail]** : affiche la base de données sur l'état des liaisons IS-IS pour les niveaux 1 et 2, ainsi que le contenu détaillé de chaque LSP.
- **show isis database verbose** : affiche plus de renseignements sur la base de données IS-IS, tels que le numéro de séquence, la somme de contrôle et le délai de rétention pour les LSP.

Supervision des entrées du tableau de mappage IS-IS

Utilisez la commande suivante pour superviser les noms d'hôte IS-IS :

show isis hostname : affiche les entrées du tableau de mappage de nom de routeur à ID système pour un routeur IS-IS.

Supervision IS-IS IPv4

Utilisez les commandes suivantes pour superviser IS-IS IPv4 :

- **show isis ip rib** : affiche la RIB spécifique à la famille d'adresses IPv4 pour un processus de routage IS-IS.
- **show isis ip spf-log** : affiche les journaux SPF spécifiques à la famille d'adresses IPv4 pour un processus de routage IS-IS.
- **show isis ip topology** : affiche la topologie spécifique à la famille d'adresses IPv4 pour un processus de routage IS-IS.
- **show isis ip redistribution** [**level-1** | **level-2**] [*network-prefix*] – Affiche les routes IPv6 IS-IS apprises et installées.
- **show isis ip unicast** : affiche la RIB, les journaux SPF et les chemins d'accès aux IS de la famille d'adresses IPv4.

Supervision IS-IS IPv6

Utilisez les commandes suivantes pour superviser IS-IS IPV6 :

- **show isis ipv6 rib** : affiche la RIB spécifique à la famille d'adresses IPv6 pour un processus de routage IS-IS.
- **show isis ipv6 spf-log** : affiche les journaux SPF spécifiques à la famille d'adresses IPv6 pour un processus de routage IS-IS.
- **show isis ipv6 topology** : affiche la topologie spécifique à la famille d'adresses IPv6 pour un processus de routage IS-IS.
- **show isis ipv6 redistribution** [**level-1** | **level-2**] [*network-prefix*] – Affiche les routes IPv6 IS-IS apprises et installées.
- **show isis ipv6 unicast** : affiche la RIB, les journaux SPF et les chemins d'accès aux IS de la famille d'adresses IPv6.

Supervision des journaux IS-IS

Utilisez les commandes suivantes pour superviser les journaux IS-IS :

- **show isis lsp-log** : affiche le journal IS-IS LSP de niveau 1 et 2 sur les interfaces qui ont déclenché le nouveau LSP.
- **show isis spf-log** : affiche la fréquence et la raison de l'exécution d'un calcul SPF par l'ASA.

Supervision du protocole IS-IS

Utilisez la commande suivante pour superviser le protocole IS-IS :

show clns protocol : affiche les renseignements sur le protocole pour chaque processus de routage IS-IS sur l'ASA.

Supervision des routes et des voisins IS-IS

Utilisez les commandes suivantes pour superviser les voisins IS-IS :

- **show isis topology** : affiche une liste de tous les routeurs connectés dans toutes les zones. Cette commande vérifie la présence et la connectivité entre tous les routeurs dans toutes les zones.
- **show isis neighbors [detail]** : affiche les renseignements de contiguïté IS-IS.
- **show clns neighbors** [*process-tag*] [*interface-name*] [**detail**] : affiche le système terminal (ES), le système intermédiaire (IS) et les voisins à topologie IS-IS (M-ISIS). Cette commande affiche la contiguïté apprise par la multitopologie IS-IS pour IPv6.
- **show clns is-neighbors** *[interface-name]* **[detail]** : affiche les renseignements IS-IS pour les contiguïtés des périphériques IS-IS.

Supervision de la RIB IS-IS

Utilisez les commandes suivantes pour superviser la RIB IS-IS :

- **show isis rib** [*ip-address* | *ip-address-mask*] : affiche les chemins pour une route donnée ou pour toutes les routes d'un réseau principal qui sont stockées dans la RIB.
- **show isis rib redistribution** [**level-1** | **level-2**] [*network-prefix*] : affiche les préfixes dans le cache de redistribution local.
- **show route isis** : affiche l'état actuel de la table de routage.

Supervision du trafic IS-IS

Utilisez la commande suivante pour superviser le trafic IS-IS :

show clns traffic [since {bootup | show}] : affiche les statistiques de trafic CLNS observées par l'ASA.

Débogage IS-IS

Utilisez les commandes suivantes pour déboguer IS-IS :

debug isis [adj-packets | authentication | checksum-errors | ip | ipv6 | local-updates | [rptpcp;-errors | rob | snp-packets | spf-events | spf-statistics | spf-triggers | update-packets] : débogue divers aspects du protocole de routage IS-IS.

Historique d'IS-IS

Tableau 42 : Historique des fonctionnalités pour IS-IS

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage IS-IS	9.6(1)	L'ASA prend désormais en charge le protocole de routage IS-IS (Intermediate System to Intermediate System). Une prise en charge a été ajoutée pour le routage des données, l'exécution de l'authentification, ainsi que la redistribution et la supervision des informations de routage à l'aide du protocole de routage IS-IS. Nous avons introduit les commandes suivantes : **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, router isis, set-attached-bit, set-overload-bit, show clns, show isis, show route isis, spf-interval, summary-address**.

Exemples d'IS-IS

Cette section décrit des exemples de configuration avec une topologie pour différents aspects d'IS-IS.

Configuration du routage IS-IS

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   isis
```

Configuration du routage IPv6 IS-IS

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   ipv6 address 2001:192:16:32::1/64
   ipv6 router isis
```

Routage dynamique dans la même zone

```
iRouter --------(inside G0/1) ASA (G0/0 outside)------------ oRouter

ASA Configuration
  interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   ipv6 address 2001:192:16:32::1/64
   isis
   ipv6 router isis

  interface GigabitEthernet0/1
   nameif inside
   security-level 100
   ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
   ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
   isis
   ipv6 router isis

  router isis
   net 49.1234.2005.2005.2005.00
   is-type level-1
   metric-style wide

  interface GigabitEthernet0/0
   ip address 172.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:16:32::3/64
   ipv6 router isis
   isis priority 120

  interface GigabitEthernet0/1
   ip address 172.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:26:32::3/64
   ipv6 router isis

IOS Configuration
  iRouter
  router isis
   net 49.1234.2035.2035.2035.00
   is-type level-1
   metric-style wide

  oRouter
  interface GigabitEthernet0/0
   ip address 192.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:192:16:32::3/64
   ipv6 router isis

  oRouter
  interface GigabitEthernet0/1
   ip address 192.26.32.3 255.255.255.0
```

```
   ip router isis
   ipv6 address 2001:192:26:32::3/64
   ipv6 router isis

  oRouter
  router isis
   net 49.1234.2036.2036.2036.00
   is-type level-1
   metric-style wide
```

Routage dynamique dans plusieurs zones

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis

 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis

 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 5
  exit-address-family
 !

IOS Configuration
 iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120


 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
```

```
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

Routage dynamique dans des zones qui se chevauchent

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis

interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
```

```
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis

router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis priority 120
 isis ipv6 metric 600


interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
 metric-style wide
 maximum-paths 6
!
 address-family ipv6
 summary-prefix 2001::/8 tag 301
 summary-prefix 6001::/16 level-1-2 tag 800
 redistribute static metric 800 level-1-2
exit-address-family


oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip pim sparse-dense-mode
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis
 isis tag 301


oRouter
```

```
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

ASA Configuration
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family
!
```

Redistribution de routes

```
iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis


 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 6
 exit-address-family
!

IOS Configuration
iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120
```

```
 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
  metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

Adresse sommaire

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis
```

```
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 redistribute static
 maximum-paths 5
address-family ipv6 unicast
 maximum-paths 6
exit-address-family
```

Interface passive

```
 iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0
  ipv6 address 2001:192:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0
  ipv6 address 2001:172:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/2
  nameif dmz
  security-level 0
  ip address 40.40.50.1 255.255.255.0
  ipv6 address 2040:95::1/64


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  passive-interface default

IOS Configuration
 iRouter
  interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120

 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
```

```
 ipv6 router isis

iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis

oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis

oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

Authentication (Authentification)

```
ASA ------------ Router

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
 ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
 ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 metric-style wide
 authentication mode md5
 authentication key cisco#123 level-2

IOS Configuration
iRouter
```

```
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis authentication mode md5
 isis authentication key-chain KeyChain level-2
 isis priority 120
 isis ipv6 metric 600


iRouter
key chain KeyChain
 key 1
  key-string cisco#123


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
```



CHAPITRE 35

EIGRP

Ce chapitre décrit comment configurer l'ASA pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole Enhanced Interior Gateway Routing Protocol (EIGRP).

- À propos d'EIGRP, à la page 1157
- Lignes directrices relatives à l'EIGRP, à la page 1159
- Configurer le protocole EIGRP, à la page 1160
- Personnaliser l'EIGRP, à la page 1162
- Supervision de l'EIGRP, à la page 1177
- Exemple pour l'EIGRP, à la page 1178
- Historique d'EIGRP, à la page 1179

À propos d'EIGRP

L'EIGRP est une version améliorée du protocole IGRP développée par Cisco. Contrairement à IGRP et RIP, EIGRP n'envoie pas de mises à jour périodiques de routage. Les mises à jour du protocole EIGRP sont envoyées uniquement lorsque la topologie du réseau change. Les principales fonctionnalités qui distinguent le protocole EIGRP des autres protocoles de routage comprennent la convergence rapide, la prise en charge des masques de sous-réseau de longueur variable, des mises à jour partielles et de plusieurs protocoles de couche réseau.

Un routeur exécutant EIGRP stocke toutes les tables de routage des voisins afin qu'il puisse s'adapter rapidement aux autres routes. Si aucune route appropriée n'existe, le protocole EIGRP interroge ses voisins pour découvrir une autre route. Ces requêtes se propagent jusqu'à ce qu'une autre route soit trouvée. Sa prise en charge pour les filtres d'adresse locale de longueur variable permet aux routes d'être récapitulées automatiquement sur une limite du nombre de réseaux. De plus, l'EIGRP peut être configuré pour résumer n'importe quelle limite de bits à n'importe quelle interface. Le protocole EIGRP ne fait pas de mises à jour périodiques. Au lieu de cela, il envoie des mises à jour partielles uniquement lorsque la mesure d'une route change. La propagation des mises à jour partielles est automatiquement limitée de sorte que seuls les routeurs qui ont besoin des renseignements sont mis à jour. En raison de ces deux fonctionnalités, EIGRP consomme beaucoup moins de bande passante qu'IGRP.

La découverte de voisin est le processus utilisé par l'ASA pour se familiariser dynamiquement avec la présence d'autres routeurs sur les réseaux directement connectés. Les routeurs EIGRP envoient des paquets Hello en multidiffusion pour annoncer leur présence sur le réseau. Lorsque l'ASA reçoit un paquet Hello d'un nouveau voisin, il envoie son tableau de topologie au voisin avec un bit d'initialisation activé. Lorsque le voisin reçoit la mise à jour de la topologie avec le bit d'initialisation activé, le voisin renvoie sa table de topologie à l'ASA.

Les paquets Hello sont envoyés en tant que messages en multidiffusion. Un message Hello n'attend aucune réponse. L'exception à cette règle concerne les voisins définis de manière statique. Si vous utilisez la commande **neighbor** ou configurez l'intervalle Hello dans ASDM pour configurer un voisin, les messages Hello envoyés à ce voisin sont envoyés en tant que messages de monodiffusion. Les mises à jour de routage et les accusés de réception sont envoyés en tant que messages de monodiffusion.

Une fois cette relation de voisin établie, les mises à jour de routage ne sont pas échangées, sauf en cas de modification de la topologie du réseau. La relation de voisin est maintenue tout au long des paquets Hello. Chaque paquet Hello reçu d'un voisin comprend un temps d'attente. Il s'agit du délai pendant lequel l'ASA peut espérer recevoir un paquet Hello de ce voisin. Si l'ASA ne reçoit pas de paquet Hello de ce voisin dans le délai de rétention annoncé par ce voisin, l'ASA considère que ce voisin n'est pas disponible.

Le protocole EIGRP utilise quatre technologies d'algorithme clés, quatre technologies clés, y compris la découverte et la récupération de voisins, le protocole RTP (Reliable Transport Protocol) et DUAL, ce qui est important pour les calculs de routes. DUAL enregistre toutes les routes vers une destination dans le tableau de topologie et non pas seulement la route la moins coûteuse. La voie de routage la moins coûteuse est insérée dans la table de routage. Les autres routages demeurent dans le tableau de topologie. En cas de défaillance de la voie principale, une autre voie est choisie parmi les successeurs possibles. Un successeur est un routeur voisin utilisé pour le transfert de paquets qui a un chemin à moindre coût vers une destination. Le calcul de faisabilité garantit que le chemin ne fait pas partie d'une boucle de routage.

Si un successeur possible n'est pas trouvé dans le tableau de topologie, un recalcul de la route doit avoir lieu. Lors du recalcul de la route, DUAL interroge les voisins EIGRP pour déterminer une route, qui à leur tour interrogent leurs voisins. Les routeurs qui n'ont pas de successeur possible pour la route renvoient un message d'inaccessibilité.

Lors du recalcul de la route, DUAL marque la route comme active. Par défaut, l'ASA attend trois minutes avant de recevoir une réponse de ses voisins. Si l'ASA ne reçoit pas de réponse d'un voisin, la route est marquée comme bloquée en mode actif. Tous les routages dans le tableau de topologie qui désignent le voisin qui ne répond pas comme un successeur de faisabilité sont supprimés.



Remarque Les relations de voisins EIGRP ne sont pas prises en charge par le tunnel IPsec sans un tunnel GRE.

Null0 et EIGRP

Par défaut, le protocole EIGRP annonce la route Null0 à l'homologue comme route récapitulative pour empêcher le routeur qui annonce le résumé de transférer des paquets n'ayant pas de route.

Par exemple, envisageons les deux routeurs, R1 et R2. Les trois interfaces sur R1 ont ces réseaux : 192.168.0.0/24, 192.168.1.0/24 et 192.168.3.0/24. Configurez R1 avec la route récapitulative 192.168.0.0/22 et annoncez-le à R2. Lorsque R2 a un paquet IP pour 192.168.2.x, il le transmettra à R1. R1 abandonnerait le paquet, car il n'a pas 192.168.2.x dans sa table de routage. Cependant, si R1 est également connecté à un FAI et qu'il a une route par défaut pointant vers le FAI, le paquet 192.168.2.x est transféré au FAI. Pour empêcher cette action de transfert, l'EIGRP génère une entrée correspondant à la route récapitulative, pointant vers Null0. Ainsi, lorsque les paquets pour 192.168.2.x sont reçus, R1 abandonnera le paquet au lieu d'utiliser la route par défaut.

Lignes directrices relatives à l'EIGRP

Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Lignes directrices relatives à la grappe

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Directives IPv6

Ne prend pas en charge IPv6.

Lignes directrices relatives au contexte

- Les instances EIGRP ne peuvent pas former de contiguïtés entre elles dans les interfaces partagées car, par défaut, l'échange inter-contextes du trafic de multidiffusion n'est pas pris en charge sur les interfaces partagées. Cependant, vous pouvez utiliser la configuration de voisin statique sous la configuration de processus EIGRP sous le processus EIGRP pour faire apparaître le voisinage EIGRP sur une interface partagée.
- L'EIGRP inter-contexte sur des interfaces distinctes est pris en charge.

Directives de redistribution

Lorsque EIGRP est configuré sur un périphérique qui fait partie du réseau OSPF ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser le routage (EIGRP ne prend pas en charge la balise de routage).

Lors de la redistribution d'EIGRP dans OSPF et d'OSPF dans EIGRP, une boucle de routage se produit en cas de panne sur une des liaisons ou interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

Directives supplémentaires

- Un maximum d'un processus EIGRP est pris en charge.
- Les intermittences de contiguïté EIGRP se produisent chaque fois qu'une modification de configuration est appliquée, ce qui entraîne une modification des renseignements de routage (envoyés ou reçus) des voisins, en particulier dans les listes de distribution, les listes de décalage et les modifications de récapitulation. Après la synchronisation des routeurs, l'EIGRP rétablit la contiguïté entre les routeurs voisins. Lorsqu'une contiguïté est supprimée et rétablie, toutes les routes apprises entre les voisins sont effacées et la synchronisation complète entre les voisins est nouvellement effectuée avec la nouvelle liste de distribution.
- Il n'y a aucune restriction sur le nombre maximum de voisins EIGRP. Cependant, pour éviter les intermittences EIGRP inutiles, nous vous conseillons de limiter le nombre à 500 par unité.

Configurer le protocole EIGRP

Cette section décrit comment activer le processus EIGRP sur votre système. Après avoir activé l'EIGRP, consultez les sections suivantes pour savoir comment personnaliser le processus EIGRP sur votre système.

Activer EIGRP

Vous ne pouvez activer qu'un seul processus de routage EIGRP sur l'ASA.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

Pour activer le processus de routage EIGRP IPv6, saisissez la commande suivante :

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Configurez les interfaces et les réseaux qui participent au routage EIGRP :

network ip-addr [mask]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Vous pouvez configurer une ou plusieurs instructions **network** avec cette commande.

Les réseaux statiques et directement connectés qui entrent dans le réseau défini sont annoncés par l'ASA. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Configurer les interfaces pour l'EIGRP, à la page 1163.

Activer le routage Stub EIGRP

Vous pouvez activer et configurer l'ASA en tant que routeur stub EIGRP. Le routage stub réduit les exigences de mémoire et de traitement sur l'ASA. En tant que routeur stub, l'ASA n'a pas besoin de maintenir une table de routage EIGRP complète, car il transfère tout le trafic non local vers un routeur de distribution. En règle générale, le routeur de distribution n'a pas besoin d'envoyer plus d'une route par défaut au routeur stub.

Seules les routes spécifiées sont propagées du routeur stub au routeur de distribution. En tant que routeur stub, l'ASA répond à toutes les requêtes de résumés, de routes connectées, de routes statiques redistribuées, de routes externes et de routes internes par le message « inaccessible ». Lorsque l'ASA est configuré en tant que stub, il envoie un paquet de renseignements sur les homologues spécial à tous les routeurs voisins pour signaler son état en tant que routeur stub. Tout voisin qui reçoit un paquet pour l'informer de l'état du stub n'interrogera pas le routeur stub sur aucune route, et un routeur qui a un homologue stub n'interrogera pas cet homologue. Le routeur stub dépend du routeur de distribution pour envoyer les mises à jour correctes à tous les homologues.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Configurez les interfaces et les réseaux qui participent au routage EIGRP :

network ip-addr [mask]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Vous pouvez configurer une ou plusieurs instructions **network** avec cette commande.

Les réseaux statiques et directement connectés qui entrent dans le réseau défini sont annoncés par l'ASA. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez la section Configurer des interfaces passives, à la page 1165.

Étape 3 Configurez le processus de routage stub :

eigrp stub {**receive-only** | [**connected**] [**redistributed**] [**static**] [**summary**]}

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# eigrp stub {receive-only | [connected] [redistributed] [static]
[summary]}
```

Vous devez spécifier quels réseaux sont annoncés par le processus de routage stub au routeur de distribution. Les réseaux statiques et connectés ne sont pas automatiquement redistribués dans le processus de routage stub.

Remarque

Un processus de routage stub ne conserve pas de table de topologie complète. Au minimum, le routage stub a besoin d'une route par défaut vers un routeur de distribution, qui prend les décisions de routage.

Personnaliser l'EIGRP

Cette section décrit comment personnaliser le routage EIGRP.

Définir un réseau pour un processus de routage EIGRP

Le tableau des réseaux vous permet de spécifier les réseaux utilisés par le processus de routage EIGRP. Pour qu'une interface participe au routage EIGRP, elle doit entrer dans la plage d'adresses définie par les entrées de réseau. Pour que les réseaux statiques et connectés directement soient annoncés, ils doivent également entrer dans la plage des entrées de réseau.

Le tableau des réseaux affiche les réseaux configurés pour le processus de routage EIGRP. Chaque ligne du tableau affiche l'adresse réseau et le masque associé configurés pour le processus de routage EIGRP indiqué.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Configurez les interfaces et les réseaux qui participent au routage EIGRP :

network ip-addr [mask]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Vous pouvez configurer une ou plusieurs instructions **network** avec cette commande.

Les réseaux statiques et directement connectés qui entrent dans le réseau défini sont annoncés par l'ASA. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Configurer des interfaces passives, à la page 1165.

Configurer les interfaces pour l'EIGRP

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est connectée à un réseau que vous souhaitez annoncer, vous pouvez configurer une commande **network** qui inclut le réseau auquel l'interface est connectée et utiliser la commande **passive-interface** pour empêcher cette interface d'envoyer ou de recevoir des mises à jour de l'EIGRP.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Configurez les interfaces et les réseaux qui participent au routage EIGRP :

network ip-addr [mask]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Vous pouvez configurer un ou plusieurs relevés de réseau avec cette commande.

Les réseaux statiques et directement connectés qui entrent dans le réseau défini sont annoncés par l'ASA. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Définir un réseau pour un processus de routage EIGRP, à la page 1162.

Étape 3 Contrôlez l'envoi ou la réception des renseignements sur la route par défaut candidate :

no default-information {**in** | **out** | **WORD**}

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

La saisie de la commande **no default-information in** entraîne le blocage du bit de route par défaut candidate sur les routes reçues.

La saisie de la commande **no default-information out** désactive le réglage du bit de route par défaut dans les routes annoncées.

Pour plus de renseignements, consultez Configurer les informations par défaut dans l'EIGRP, à la page 1174

Étape 4 Activez l'authentification MD5 des paquets EIGRP :

authentication mode eigrp as-num **md5**

Exemple :

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP configuré sur l'ASA. Si l'EIGRP n'est pas activé ou si vous saisissez le mauvais numéro, l'ASA renvoie le message d'erreur suivant :

```
% Asystem(100) specified does not exist
```

Pour obtenir plus de renseignements, consultez Activer l'authentification EIGRP sur une interface, à la page 1167.

Étape 5 Définissez la valeur du délai :

delay *value*

Exemple :

```
ciscoasa(config-if)# delay 200
```

L'argument *value* saisi est exprimé en dixièmes de microsecondes. Pour définir le délai de 2 000 microsecondes, entrez une *valeur* de 200.

Pour afficher la valeur de délai attribuée à une interface, utilisez la commande **show interface**.

Pour en savoir plus, consultez Modifier la valeur du délai d'interface, à la page 1166.

Étape 6 Modifiez l'intervalle Hello :

hello-interval eigrp as-num seconds

Exemple :

```
ciscoasa(config)# hello-interval eigrp 2 60
```

Pour obtenir plus de renseignements, consultez Personnaliser l'intervalle Hello et le délai de rétention dans l'EIGRP, à la page 1173.

Étape 7 Modifiez le délai de rétention :

hold-time eigrp as-num seconds

Exemple :

```
ciscoasa(config)# hold-time eigrp 2 60
```

Pour obtenir plus de renseignements, consultez Personnaliser l'intervalle Hello et le délai de rétention dans l'EIGRP, à la page 1173.

Configurer des interfaces passives

Vous pouvez configurer une ou plusieurs interfaces en tant qu'interfaces passives. Dans EIGRP, une interface passive n'envoie ni ne reçoit de mises à jour de routage.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Configurez les interfaces et les réseaux qui participent au routage EIGRP. Vous pouvez configurer un ou plusieurs relevés **network** avec cette commande.

network ip-addr [mask]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Les réseaux statiques et directement connectés qui entrent dans le réseau défini sont annoncés par l'ASA. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Définir un réseau pour un processus de routage EIGRP, à la page 1162.

Étape 3 Empêchez une interface d'envoyer ou de recevoir un message de routage EIGRP :

passive-interface {**default** | if-name}

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# passive-interface {default}
```

L'utilisation du mot clé **default** désactive les mises à jour de routage EIGRP sur toutes les interfaces. La définition d'un nom d'interface, comme défini par la commande **nameif**, désactive les mises à jour de routage

EIGRP sur l'interface spécifiée. Vous pouvez utiliser plusieurs commandes **passive-interface** dans la configuration de votre routeur EIGRP.

Configurer les adresses d'agrégation du résumé sur les interfaces

Vous pouvez configurer une adresse sommaire pour chaque interface. Vous devez définir manuellement les adresses sommaires si vous souhaitez créer des adresses sommaires qui ne se produisent pas à la limite d'un numéro de réseau, ou si vous souhaitez utiliser des adresses sommaires sur l'ASA avec le récapitulatif de routage automatique désactivé. Si des routes plus spécifiques se trouvent dans la table de routage, EIGRP annoncera l'adresse sommaire hors de l'interface avec une mesure égale au minimum de toutes les routes plus spécifiques.

Procédure

Étape 1 Entrez en mode de configuration d'interface pour l'interface sur laquelle vous modifiez la valeur du délai utilisée par l'EIGRP :

interface phy_if

Exemple :

```
ciscoasa(config)# interface inside
```

Étape 2 Créez l'adresse sommaire :

summary-address eigrp *as-num address mask* [*distance*]

Exemple :

```
ciscoasa(config-if)# summary-address eigrp 2 address mask [20]
```

Par défaut, les adresses sommaires EIGRP que vous définissez ont une distance administrative de 5. Vous pouvez modifier cette valeur en spécifiant l'argument *distance* facultatif dans la commande **summary-address**.

Modifier la valeur du délai d'interface

La valeur du délai d'interface est utilisée dans les calculs de distance EIGRP. Vous pouvez modifier cette valeur par interface.

Procédure

Étape 1 Entrez en mode de configuration d'interface pour l'interface sur laquelle vous modifiez la valeur du délai utilisée par l'EIGRP :

interface phy_if

Exemple :

```
ciscoasa(config)# interface inside
```

Étape 2 Définissez une valeur de délai :

delay *value*

Exemple :

```
ciscoasa(config-if)# delay 200
```

L'argument *value* saisi est exprimé en dixièmes de microsecondes. Pour définir le délai de 2 000 microsecondes, vous entrez une *valeur* de 200.

Remarque
Pour afficher la valeur de délai attribuée à une interface, utilisez la commande **show interface**.

Activer l'authentification EIGRP sur une interface

L'authentification de route EIGRP fournit une authentification MD5 des mises à jour de routage provenant du protocole de routage EIGRP. Le condensé de clé MD5 dans chaque paquet EIGRP empêche l'introduction de messages de routage non autorisés ou faux provenant de sources non approuvées.

L'authentification de route EIGRP est configurée par interface. Tous les voisins EIGRP sur les interfaces configurées pour l'authentification des messages EIGRP doivent être configurés avec le même mode d'authentification et la même clé pour que les contiguïtés soient établies.



Remarque Avant de pouvoir activer l'authentification de routage EIGRP, vous devez activer EIGRP.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp *as-num*

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument as-num est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Configurez les interfaces et les réseaux qui participent au routage EIGRP :

network *ip-addr* [*mask*]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

- Vous pouvez configurer un ou plusieurs relevés de réseau avec cette commande.
- Les réseaux statiques et directement connectés qui entrent dans le réseau défini sont annoncés par l'ASA. De plus, seules les interfaces ayant une adresse IP comprise dans le réseau défini participent au processus de routage EIGRP.
- Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Configurer le protocole EIGRP, à la page 1160.

Étape 3 Entrez en mode de configuration d'interface pour l'interface sur laquelle vous configurez l'authentification du message EIGRP :

interface *phy_if*

Exemple :

```
ciscoasa(config)# interface inside
```

Étape 4 Activez l'authentification MD5 des paquets EIGRP :

authentication mode eigrp *as-num* md5

Exemple :

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

L'argument as-num est le numéro de système autonome du processus de routage EIGRP configuré sur l'ASA. Si l'EIGRP n'est pas activé ou si vous saisissez le mauvais numéro, l'ASA renvoie le message d'erreur suivant :

```
% Asystem(100) specified does not exist
```

Étape 5 Configurez la clé utilisée par l'algorithme MD5 :

authentication key eigrp *as-num key* key-id *key-id*

Exemple :

```
ciscoasa(config)# authentication key eigrp 2 cisco key-id 200
```

- L'argument as-num est le numéro de système autonome du processus de routage EIGRP configuré sur l'ASA. Si l'EIGRP n'est pas activé ou si vous saisissez le mauvais numéro, l'ASA renvoie le message d'erreur suivant :

```
% Asystem(100) specified does not exist%
```

- L'argument key peut inclure jusqu'à 16 caractères, y compris des lettres, des chiffres et des caractères spéciaux. Les espaces blancs ne sont pas autorisés dans l'argument key.
- L'argument key-id est un nombre compris entre 0 et 255.

Définir un voisin EIGRP

Les paquets Hello EIGRP sont envoyés en tant que paquets de multidiffusion. Si un voisin EIGRP se trouve sur un réseau de non-diffusion, comme un tunnel, vous devez définir manuellement ce voisin. Lorsque vous définissez manuellement un voisin EIGRP, les paquets Hello sont envoyés à ce voisin sous forme de messages de monodiffusion.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Configurez les interfaces et les réseaux qui participent au routage EIGRP :

network ip-addr [mask]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Étape 3 Définissez le voisin statique :

neighbor *ip-addr* **interface** *if_name*

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

L'argument *ip-addr* est l'adresse IP du voisin.

L'argument *if-name* est le nom de l'interface, tel que spécifié par la commande **nameif**, par l'intermédiaire de laquelle ce voisin est disponible. Vous pouvez définir plusieurs voisins pour un processus de routage EIGRP.

Remarque

Vous devez configurer le réseau d'interfaces qui participent au routage EIGRP pour que la configuration de voisinage soit effective.

Redistribuer les routes dans l'EIGRP

Vous pouvez redistribuer les routes détectées par RIP et OSPF dans le processus de routage EIGRP. Vous pouvez également redistribuer les routes statiques et connectées dans le processus de routage EIGRP. Vous n'avez pas besoin de redistribuer les routes connectées si elles entrent dans la plage d'une instruction **network** dans la configuration EIGRP.



Remarque Pour le protocole RIP uniquement : avant d'entamer cette procédure, vous devez créer une carte de routage pour définir plus précisément quelles routes du protocole de routage spécifié sont redistribuées dans le processus de routage RIP.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 (Facultatif) Spécifie les mesures par défaut qui doivent être appliquées aux routes redistribuées dans le processus de routage EIGRP :

default-metric : MTU de chargement de la fiabilité du délai de bande passante

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu
```

Si vous ne spécifiez pas de mesure par défaut dans la configuration du routeur EIGRP, vous devez préciser les valeurs de mesure dans chaque commande **redistribute**. Si vous spécifiez les mesures EIGRP dans la commande **redistribute** et que vous avez la commande **default-metric** dans la configuration du routeur EIGRP, les mesures de la commande **redistribute** sont utilisées.

Étape 3 Redistribuez les routes connectées dans le processus de routage EIGRP :

redistribute connected [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

Exemple :

```
ciscoasa(config-router)# redistribute connected [metric bandwidth delay reliability loading
 mtu] [route-map map_name]
```

Vous devez spécifier les valeurs de la mesure EIGRP dans la commande **redistribute** si vous n'avez pas de commande **default-metric** dans la configuration du routeur EIGRP.

Étape 4 Redistribuez les routes statiques dans le processus de routage EIGRP :

redistribute static [**route-map** map_name]

Exemple :

```
ciscoasa(config-router)# redistribute static [route-map map_name]
```

Cette commande transmettra toutes les routes statiques à l'EIGRP. Pour redistribuer les routes statiques sélectives, assurez-vous de créer une liste d'accès avec la route statique, puis de l'inclure dans une carte de routage :

Exemple :

```
ciscoasa(config)# ip access-list extended R1_Loopback
ciscoasa(config-ext-nacl)#permit ip host 1.1.1.1 any
ciscoasa(config-ext-nacl)#exit

ciscoasa(config)#route-map Permit_to_Distribute
ciscoasa(config-route-map)#match ip address R1_Loopback
ciscoasa(config-route-map)#exit
```

Après avoir créé la carte de routage, incluez-la dans la commande de redistribution comme suit :

Exemple :

```
ciscoasa(config)#router eigrp 2
ciscoasa(config-router)#redistribute static subnets route-map Permit_to_Distribute
```

Étape 5 Redistribuez les routes d'un processus de routage OSPF dans le processus de routage EIGRP :

redistribute ospf pid [**match** {**internal | external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

Exemple :

```
ciscoasa(config-router): redistribute ospf pid [match {internal | external [1 | 2] |
nssa-external [1 | 2]}] [metric bandwidth delay reliability loading mtu] [route-map map_name]
```

Étape 6 Redistribuez les routes d'un processus de routage RIP dans le processus de routage EIGRP :

redistribute rip [**metric** bandwidth delay reliability load mtu] [**route-map map_name**]

Exemple :

```
ciscoasa(config-router): redistribute rip [metric bandwidth delay
reliability load mtu] [route-map map_name]
```

Filtrer les réseaux dans l'EIGRP

Remarque Avant de commencer ce processus, vous devez créer une ACL standard qui définit les routes que vous souhaitez annoncer. C'est-à-dire que vous créez une ACL standard qui définit les routes que vous souhaitez filtrer à partir de l'envoi ou de la réception des mises à jour.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Configurez les interfaces et les réseaux qui participent au routage EIGRP :

ciscoasa(config-router)# **network** ip-addr [mask]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Vous pouvez configurer un ou plusieurs relevés de réseau avec cette commande.

Les réseaux statiques et directement connectés qui entrent dans le réseau défini sont annoncés par l'ASA. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Configurer les interfaces pour l'EIGRP, à la page 1163.

Étape 3 Filtrez les réseaux envoyés dans les mises à jour du routage EIGRP :

distribute-list acl **out** [**connected** | **ospf** | **rip** | **static** | **interface** if_name]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl out [connected]
```

Vous pouvez définir une interface pour appliquer le filtre uniquement aux mises à jour envoyées par cette interface en particulier.

Vous pouvez saisir plusieurs commandes **distribute-list** dans la configuration de votre routeur EIGRP.

Étape 4 Filtrez les réseaux reçus dans les mises à jour du routage EIGRP :

distribute-list acl **in** [**interface** if_name]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl in [interface interface1]
```

Vous pouvez définir une interface pour appliquer le filtre uniquement aux mises à jour reçues par cette interface.

Personnaliser l'intervalle Hello et le délai de rétention dans l'EIGRP

L'ASA envoie périodiquement des paquets Hello pour découvrir les voisins et savoir quand ceux-ci deviennent inaccessibles ou inopérants. Par défaut, les paquets Hello sont envoyés toutes les 5 secondes.

Le paquet Hello annonce le délai de rétention de l'ASA. Le délai de rétention indique aux voisins EIGRP la durée pendant laquelle le voisin doit considérer l'ASA comme accessible. Si le voisin ne reçoit pas de paquet Hello dans le délai de rétention annoncé, l'ASA est considéré comme inaccessible. Par défaut, le délai de rétention annoncé est de 15 secondes (trois fois l'intervalle Hello).

L'intervalle Hello et le délai de rétention annoncé sont configurés par interface. Nous vous conseillons de définir le délai de rétention à au moins trois fois l'intervalle Hello.

Procédure

Étape 1 Entrez en mode de configuration d'interface pour l'interface sur laquelle vous configurez l'intervalle Hello ou le délai de rétention annoncé :

interface phy_if

Exemple :

```
ciscoasa(config)# interface inside
```

Étape 2 Modifiez l'intervalle Hello :

hello-interval eigrp as-num seconds

Exemple :

```
ciscoasa(config)# hello-interval eigrp 2 60
```

Étape 3 Modifiez le délai de rétention :

hold-time eigrp as-num seconds

Exemple :

```
ciscoasa(config)# hold-time eigrp 2 60
```

Désactiver la synthèse automatique des routes

La synthèse automatique des routes est activée par défaut. Le processus de routage par EIGRP se résume sur les limites des numéros de réseau. Cela eut entraîner des problèmes de routage si vous avez des réseaux non contigus.

Par exemple, si vous avez un routeur avec les réseaux 192.168.1.0, 192.168.2.0 et 192.168.3.0 qui y sont connectés et que ces réseaux participent tous à l'EIGRP, le processus de routage EIGRP crée l'adresse sommaire 192.168.0.0 pour ces routes. Si un routeur supplémentaire est ajouté au réseau avec les réseaux 192.168.10.0 et 192.168.11.0 et que ces réseaux participent à l'EIGRP, ils seront également résumés sous la forme 192.168.0.0. Pour éviter que le trafic ne soit acheminé vers le mauvais emplacement, vous devez désactiver la synthèse automatique des routes sur les routeurs qui créent des adresses sommaires conflictuelles.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Désactivez la synthèse automatique des routes :

no auto-summary

Exemple :

```
ciscoasa(config-router)# no auto-summary
```

Les adresses sommaires automatiques ont une distance administrative par défaut de 5.

Configurer les informations par défaut dans l'EIGRP

Vous pouvez contrôler l'envoi et la réception des renseignements sur la route par défaut dans les mises à jour EIGRP. Par défaut, les routes par défaut sont envoyées et acceptées. La configuration de l'ASA pour interdire la réception des renseignements par défaut entraîne le blocage du bit de route par défaut possible sur les routes reçues. La configuration de l'ASA pour interdire l'envoi des renseignements par défaut désactive le réglage du bit de route par défaut dans les routes annoncées.

Procédure

Étape 1 Créez un processus de routage EIGRP et passez en mode de configuration du routeur pour ce processus EIGRP :

router eigrp as-num

Exemple :

```
ciscoasa(config)# router eigrp 2
```

L'argument *as-num* est le numéro de système autonome du processus de routage EIGRP.

Étape 2 Configurez les interfaces et les réseaux qui participent au routage EIGRP :

network ip-addr [mask]

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Vous pouvez configurer un ou plusieurs relevés de réseau avec cette commande.

Les réseaux statiques et directement connectés qui entrent dans le réseau défini sont annoncés par l'ASA. De plus, seules les interfaces ayant une adresse IP qui entre dans le réseau défini participent au processus de routage EIGRP.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage EIGRP, mais qui est associée à un réseau que vous souhaitez annoncer, consultez Configurer les interfaces pour l'EIGRP, à la page 1163.

Étape 3 Contrôlez l'envoi ou la réception des renseignements sur la route par défaut candidate :

no default-information {**in** | **out** | **WORD**}

Exemple :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

Remarque
La saisie de la commande **no default-information in** entraîne le blocage du bit de route par défaut candidate sur les routes reçues. La saisie de la commande **no default-information out** désactive le réglage du bit de route par défaut dans les routes annoncées.

Désactiver l'horizon divisé de l'EIGRP

L'horizon partagé contrôle l'envoi des paquets de mise à jour et de requête de l'EIGRP. Lorsque l'horizon partagé est activé sur une interface, les paquets de mise à jour et de requête ne sont pas envoyés vers les

destinations pour lesquelles cette interface est le prochain saut. Le contrôle des paquets de mise à jour et de requête de cette manière réduit le risque de boucles de routage.

Par défaut, l'horizon partagé est activé sur toutes les interfaces.

L'horizon partagé empêche les renseignements de routage d'être annoncés par un routeur à partir de toute interface d'où proviennent ces renseignements. Ce comportement optimise généralement les communications entre plusieurs périphériques de routage, en particulier lorsque des liaisons sont rompues. Cependant, avec les réseaux de non-diffusion, il peut arriver que ce comportement ne soit pas souhaitable. Pour ces situations, y compris les réseaux dans lesquels vous avez configuré l'EIGRP, vous pouvez désactiver l'horizon partagé.

Si vous désactivez l'horizon partagé sur une interface, vous devez le désactiver pour tous les routeurs et les serveurs d'accès sur cette interface.

Pour désactiver l'horizon partagé de l'EIGRP, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration d'interface pour l'interface sur laquelle vous modifiez la valeur du délai utilisée par l'EIGRP :

interface phy_if

Exemple :

```
ciscoasa(config)# interface phy_if
```

Étape 2 Désactivez l'horizon partagé :

no split-horizon eigrp *as-number*

Exemple :

```
ciscoasa(config-if)# no split-horizon eigrp 2
```

Redémarrer le processus EIGRP

Vous pouvez redémarrer un processus EIGRP ou effacer la redistribution ou les compteurs.

Procédure

Redémarrez un processus EIGRP ou effacez la redistribution ou les compteurs :

clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events)**}

Exemple :

```
ciscoasa(config)# clear eigrp pid 10 neighbors
```

Supervision de l'EIGRP

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage EIGRP. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande. En outre, vous pouvez désactiver la journalisation des messages de modification de voisin et des messages d'avertissement de voisin.

Pour superviser ou désactiver diverses statistiques de routage EIGRP, saisissez l'une des commandes suivantes :

- **router-id**

  Affiche l'ID de routeur pour ce processus EIGRP.

- **show eigrp** [*as-number*] **events** [{*start end*} | **type**]

  Affiche le journal des événements EIGRP.

- **show eigrp** [*as-number*] **interfaces** [*if-name*] [**detail**]

  Affiche les interfaces participant au routage EIGRP.

- **show eigrp** [as-number] **neighbors** [**detail** | **static**] [*if-name*]

  Affiche le tableau des voisins EIGRP.

- **show eigrp** [*as-number*] **topology** [*ip-addr* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  Affiche le tableau de topologie du EIGRP.

- **show eigrp** [*as-number*] **traffic**

  Affiche les statistiques de trafic EIGRP.

- **show mfib cluster**

  Affiche les renseignements MFIB en termes d'entrées et d'interfaces de transfert.

- **show route cluster**

  Affiche des détails supplémentaires sur la synchronisation des routes pour la mise en grappe.

- **no eigrp log-neighbor-changes**

  Désactive la journalisation des messages de modification de voisin. Saisissez cette commande en mode de configuration du routeur pour le processus de routage EIGRP.

- **no eigrp log-neighbor-warnings**

  Désactive la journalisation des messages d'avertissement de voisin.

- **show ipv6 eigrp** *as-number* **interface** *interface*

  Affiche le tableau de topologie EIGRP IPv6.

- **show ipv6 eigrp** [*as-number*] **traffic**

  Affiche les statistiques de trafic EIGRP IPv6.

- **show ipv6 eigrp** [as-number] **neighbors** [*if-name*]

  Affiche le tableau des voisins EIGRP IPv6.

- **show ipv6 eigrp interfaces** [*if-name*]

  Affiche les renseignements relatifs au voisin pour une interface donnée.

- **show ipv6 eigrp** [*as-number*] **topology** [*ipv6-address* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  Affiche le tableau de topologie EIGRP IPv6.

- **show ipv6 eigrp** [*as-number*] **events** [{*start* - *end*} | **type**]

  Affiche le journal des événements EIGRP IPv6.

- **show ipv6 eigrp timers**

  Affiche la minuterie Hello et le délai de rétention configurés.

Exemple pour l'EIGRP

L'exemple suivant montre comment activer et configurer EIGRP avec différents processus facultatifs :

Procédure

Étape 1 Pour activer EIGRP, saisissez les commandes suivantes :

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Étape 2 Pour configurer une interface à partir de l'envoi ou de la réception de messages de routage EIGRP, saisissez la commande suivante :

```
ciscoasa(config-router)# passive-interface {default}
```

Étape 3 Pour définir un voisin EIGRP, saisissez la commande suivante :

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

Étape 4 Pour configurer les interfaces et les réseaux qui participent au routage EIGRP, saisissez la commande suivante :

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

Étape 5 Pour modifier la valeur de délai d'interface utilisée dans les calculs de distance EIGRP, saisissez les commandes suivantes :

```
ciscoasa(config-router)# exit
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# delay 200
```

Historique d'EIGRP

Tableau 43 : Historique des fonctionnalités d'EIGRP

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge d'EIGRP	7.0(1)	Une prise en charge a été ajoutée pour le routage des données, l'exécution de l'authentification, ainsi que la redistribution et la supervision des informations de routage à l'aide du protocole EIGRP (Enhanced Interior Gateway Routing Protocol). Nous avons introduit la commande suivante : **route eigrp**.
Routage dynamique en mode de contexte multiple	9.0(1)	Le routage EIGRP est pris en charge en mode de contexte multiple.
Mise en grappe	9.0(1)	Pour l'EIGRP, la synchronisation groupée, la synchronisation du routage et l'équilibrage de charges de couche 2 sont pris en charge dans l'environnement de mise en grappe. Nous avons introduit ou modifié les commandes suivantes : **show route cluster**, **debug route cluster, show mfib cluster, debug mfib cluster**.
Champ Auto-Summary (Résumé automatique) de l'EIGRP	9.2(1)	Pour l'EIGRP, le champ Auto-Summary (Résumé automatique) est maintenant désactivé par défaut.



CHAPITRE 36

Routage multidiffusion

Ce chapitre décrit comment configurer ASA pour utiliser le protocole de routage de multidiffusion.

- À propos du routage de multidiffusion, à la page 1181
- Lignes directrices pour le routage de multidiffusion, à la page 1184
- Routage multidiffusion activé, à la page 1185
- Personnaliser le routage multidiffusion, à la page 1186
- Supervision de PIM, à la page 1198
- Exemple de routage de multidiffusion, à la page 1199
- Historique du routage de multidiffusion, à la page 1200

À propos du routage de multidiffusion

Le routage de multidiffusion est une technologie de conservation de la bande passante qui réduit le trafic en délivrant simultanément un seul flux d'informations à des milliers d'entreprises et de domiciles. Les applications qui tirent parti du routage de multidiffusion comprennent les vidéoconférences, les communications d'entreprise, l'apprentissage à distance et la distribution de logiciels, de cotations boursières et d'actualités.

Les protocoles de routage de multidiffusion acheminent le trafic source vers plusieurs récepteurs sans ajouter de charge supplémentaire pour la source ou les récepteurs, tout en utilisant la moindre bande passante de réseau de toutes les technologies concurrentes. Les paquets en multidiffusion sont répliqués dans le réseau par l'activation de ASA avec PIM (Protocol Independent Multicast) et d'autres protocoles de multidiffusion qui prennent en charge, ce qui permet la livraison la plus efficace possible des données à plusieurs destinataires.

L'ASA prend en charge le routage de multidiffusion stub et le routage de multidiffusion PIM. Cependant, vous ne pouvez pas configurer les deux simultanément sur un seul ASA.

Remarque Les transports UDP et non-UDP sont tous deux pris en charge pour le routage de multidiffusion. Cependant, le transport non UDP n'a pas d'optimisation FastPath.

Routage de multidiffusion Stub

Le routage de multidiffusion tampon permet un enregistrement dynamique de l'hôte et facilite le routage de multidiffusion. Lorsqu'il est configuré pour le routage de multidiffusion stub, l'ASA agit comme un agent mandataire IGMP. Au lieu de participer entièrement au routage de multidiffusion, l'ASA transfère les messages

IGMP à un routeur de multidiffusion en amont, qui configure la livraison des données en multidiffusion. Lorsqu'il est configuré pour le routage de multidiffusion tampon, l'ASA ne peut pas être configuré pour le mode PIM discret ou bidirectionnel. Vous devez activer PIM sur les interfaces qui participent au routage de la multidiffusion en mode stub IGMP.

L'ASA prend en charge PIM-SM et PIM bidirectionnel. PIM-SM est un protocole de routage de multidiffusion qui utilise la base d'information de routage sous-jacente de monodiffusion ou une base d'information de routage distincte compatible avec la multidiffusion. Il crée des arborescences partagées unidirectionnelles enracinées à un seul point RP (Rendez-vous point) par groupe de multidiffusion et crée éventuellement des arborescences du chemin le plus court par source de multidiffusion.

Routage de multidiffusion PIM

Le PIM bidirectionnel est une variante de PIM-SM qui crée des arborescences partagées bidirectionnelles connectant les sources et les récepteurs de multidiffusion. Les arborescences bidirectionnelles sont créées à l'aide d'un processus de sélection de désigné de transitaire (DF) qui fonctionne sur chaque lien de la topologie de multidiffusion. Avec l'aide du DF, les données en multidiffusion sont transmises des sources au point de rendez-vous (RP), et donc le long de l'arborescence partagée jusqu'aux récepteurs, sans nécessiter d'état propre à la source. Le choix du DF a lieu lors de la découverte du RP et fournit une voie de routage par défaut vers le RP.



Remarque Si ASA est le RP du PIM, utilisez l'adresse externe non traduite du ASA comme adresse RP.

Prise en charge de la multidiffusion PIM propre à la source

L'ASA ne prend pas en charge la fonctionnalité PIM de multidiffusion source spécifique (SSM) et la configuration associée. Cependant, l'ASA permet aux paquets liés au SSM de passer, sauf s'il est placé comme routeur de dernier saut.

SSM est classé comme un mécanisme de livraison de données pour les applications un-à-plusieurs telles que l'IPTV. Le modèle SSM utilise un concept de « canaux » désigné par une paire (S, G), où S est une adresse de source et G une adresse de destination SSM. L'abonnement à un canal se fait à l'aide d'un protocole de gestion de groupe comme IGMPv3. SSM permet à un client destinataire, une fois qu'il a pris connaissance d'une source en multidiffusion particulière, de recevoir des flux en multidiffusion directement de la source plutôt que de les recevoir d'un point de rendez-vous partagé (RP). Des mécanismes de contrôle d'accès ont été introduits dans SSM pour fournir une amélioration de la sécurité non disponible avec les implémentations actuelles en mode clairsemé ou dense.

PIM-SSM diffère de PIM-SM en ce qu'il n'utilise pas de RP ou d'arborescence partagée. Au lieu de cela, les informations sur les adresses de sources d'un groupe de multidiffusion sont fournies par les récepteurs au moyen du protocole IGMPv3) et sont utilisées pour créer directement des arborescences propres aux sources.

Routeur de démarrage PIM (BSR)

PIM Bootstrap Router (BSR) est un modèle de sélection dynamique des Points de Rendez vous (RP) qui utilise des routeurs candidats pour la fonction RP et pour le relais des informations RP pour un groupe. La fonction RP comprend la découverte de RP et fournit une voie de routage par défaut vers le RP. Pour ce faire, elle configure un ensemble de périphériques en tant que candidats BSR (C-BSR) qui participent à un processus de sélection d'un BSR pour choisir un BSR parmi eux. Une fois le BSR choisi, les périphériques configurés

en tant que points de rendez-vous candidats (C-RP) commencent à envoyer leur mappage de groupe au BSR élu. Le BSR distribue ensuite les informations de mappage groupe-RP à tous les autres périphériques en aval dans l'arborescence de multidiffusion par l'intermédiaire de messages du BSR qui voyagent de routeur PIM à routeur PIM par saut.

Cette fonctionnalité fournit un moyen d'apprendre dynamiquement les RP, ce qui est tout à fait essentiel dans les grands réseaux complexes où un RP peut périodiquement tomber en panne et se relancer.

Terminologie du routeur de démarrage PIM (BSR)

Les termes suivants sont fréquemment mentionnés dans la configuration du BSR PIM :

- Routeur Bootstrap (BSR) : un BSR annonce des informations de point de rendez-vous (RP) à d'autres routeurs avec PIM saut par saut. Parmi plusieurs candidats BSR, un seul BSR est choisi à l'issu d'un processus de sélection. L'objectif principal de ce routeur Bootstrap est de collecter toutes les annonces de Candidat RP (C-RP) dans une base de données appelée RP-set et de les envoyer périodiquement à tous les autres routeurs du réseau en tant que messages BSR (toutes les 60 secondes) .
- Messages Bootstrap Router (BSR) : les messages BSR sont en multidiffusion vers le groupe All-PIM-Routers avec une TTL de 1. Tous les voisins PIM qui reçoivent ces messages les retransmettent (encore une fois avec une TTL de 1) sur toutes les interfaces, à l'exception de celle dans laquelle les messages ont été reçus. Les messages BSR contiennent l'ensemble de RP et l'adresse IP du BSR actuellement actif. Voici comment les C-RP savent où envoyer en monodiffusion leurs messages C-RP.
- Candidate Bootstrap Router (C-BSR) : un appareil configuré en tant que candidat-BSR participe au mécanisme de sélection du BSR. Un C-BSR de priorité la plus élevée est choisi comme BSR. L'adresse IP la plus élevée de C-BSR est utilisée comme condition de départage. Le processus de sélection BSR est préemptif, par exemple, si un nouveau C-BSR avec une priorité plus élevée se présente, il déclenche un nouveau processus de sélection.
- Point de rendez-vous candidat (C-RP) : un RP sert de point de rencontre pour les sources et les récepteurs des données de multidiffusion. Un périphérique configuré en tant que C-RP annonce périodiquement les informations de mappage de groupe de multidiffusion directement au BSR choisi par la monodiffusion. Ces messages contiennent la plage de groupe, l'adresse C-RP et une durée d'attente. L'adresse IP du BSR actuel est apprise à partir des messages périodiques du BSR reçus par tous les routeurs du réseau. De cette façon, le BSR apprend quels sont les RP possibles qui sont actuellement actifs et accessibles.



Remarque L'ASA n'agit pas comme un C-RP, même si le C-RP est une exigence obligatoire pour le trafic BSR. Seuls les routeurs peuvent agir en tant que C-RP. Ainsi, pour la fonctionnalité de test du BSR, vous devez ajouter des routeurs à la topologie.

- Mécanisme de sélection BSR – Chaque C-BSR génère des messages Bootstrap (BSM) qui contiennent un champ de priorité BSR. Les routeurs du domaine inondent les BSM dans tout le domaine. Un C-BSR qui entend parler d'un C-BSR de priorité plus élevée que lui supprime l'envoi d'autres BSM pendant un certain temps. L'unique C-BSR restant devient le BSR élu, et ses BSM informent tous les autres routeurs du domaine qu'il est le BSR choisi.

Concept de groupe de multidiffusion

La multidiffusion est basée sur le concept de groupe. Un groupe arbitraire de récepteurs souhaite recevoir un flux de données particulier. Ce groupe n'a aucune frontière physique ou géographique : les hôtes peuvent être situés n'importe où sur Internet. Les hôtes qui souhaitent recevoir des données vers un groupe en particulier doivent rejoindre ce groupe au moyen d'IGMP. Les hôtes doivent être membres du groupe pour recevoir le flux de données.

Adresses de multidiffusion

Les adresses de multidiffusion spécifient un groupe quelconque d'hôtes IP qui ont rejoint le groupe et qui souhaitent recevoir le trafic envoyé à ce groupe.

Mise en grappe

Le routage de multidiffusion prend en charge la mise en grappe. Dans la mise en grappe étendue EtherChannel, l'unité de contrôle envoie tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi. Une fois le transfert rapide établi, les unités de données peuvent transférer des paquets de données en multidiffusion. Tous les flux de données sont des flux complets. Les flux de transfert des tampons sont également pris en charge. Comme une seule unité reçoit les paquets en multidiffusion dans une grappe EtherChannel étendue, la redirection vers l'unité de contrôle est courante. Dans le regroupement d'interfaces individuelles, les unités n'agissent pas indépendamment. Toutes les données et les paquets de routage sont traités et transmis par l'unité de contrôle. Les unités de données abandonnent tous les paquets qui ont été envoyés.

Lignes directrices pour le routage de multidiffusion

Mode contextuel

Pris en charge en mode contexte unique

Mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

IPv6

Ne prend pas en charge IPv6.

Groupe de multidiffusion

La plage d'adresses entre 224.0.0.0 et 224.0.0.255 est réservée pour l'utilisation des protocoles de routage et d'autres protocoles de découverte ou de maintenance de topologie, tels que la découverte de passerelle et les rapports sur les membres de groupes. Par conséquent, le routage de multidiffusion Internet à partir de la plage d'adresses 224.0.0/24 n'est pas pris en charge; Le groupe IGMP n'est pas créé lors de l'activation du routage de multidiffusion pour les adresses réservées.

Mise en grappe

En grappe, pour IGMP et PIM, cette fonctionnalité n'est prise en charge que sur l'unité principale.

Directives supplémentaires

- Vous devez configurer une règle de contrôle d'accès sur l'interface entrante pour autoriser le trafic vers l'hôte de multidiffusion, comme l'interface 224.1.2.3. Cependant, vous ne pouvez pas spécifier une interface de destination pour la règle, ou elle ne peut pas être appliquée aux connexions en multidiffusion lors de la validation initiale de la connexion.
- Le routage de multidiffusion PIM/IGMP n'est pas pris en charge sur les interfaces dans une zone de trafic.
- Ne configurez pas ASA pour être à la fois un point de rendez-vous (RP) et un routeur de premier saut.
- L'adresse IP de secours HSRP ne participe pas au voisinage PIM. Ainsi, si l'adresse IP du routeur RP est acheminée par l'intermédiaire d'une adresse IP de secours HSRP, le routage de multidiffusion ne fonctionne pas dans ASA. Par conséquent, pour que le trafic en multidiffusion réussisse, assurez-vous que la voie de routage pour l'adresse RP n'est pas l'adresse IP de secours HSRP. Configurez plutôt l'adresse de routage sur une adresse IP d'interface.

Routage multidiffusion activé

L'activation du routage de multidiffusion sur l'ASA active l'IGMP et la PIM sur toutes les interfaces de données par défaut, mais pas sur l'interface de gestion pour la plupart des modèles (voir L'interface de logement/port de gestion, à la page 672 pour les interfaces qui n'autorisent pas le trafic). IGMP est utilisé pour savoir si les membres d'un groupe sont présents sur les sous-réseaux directement associés. Les hôtes se joignent aux groupes de multidiffusion en envoyant des messages de rapport IGMP. PIM est utilisé pour maintenir les tableaux de transfert pour transférer les datagrammes en multidiffusion.

Pour activer le routage de multidiffusion sur l'interface de gestion, vous devez définir explicitement une limite de multidiffusion sur l'interface de gestion.

Remarque Seule la couche de transport UDP est prise en charge pour le routage de multidiffusion.

La liste suivante indique le nombre maximal d'entrées pour des tableaux de multidiffusion spécifiques. Une fois ces limites atteintes, toute nouvelle entrée est rejetée.

- MFIB : 30 000
- Groupes IGMP : 30 000
- Routages PIM : 72 000

Procédure

Activez le routage de multidiffusion :

multicast-routing

Exemple :

```
ciscoasa(config)# multicast-routing
```

Le nombre d'entrées dans les tables de routage de multidiffusion est limité par la quantité de RAM sur l'ASA.

Personnaliser le routage multidiffusion

Cette section décrit comment personnaliser le routage multidiffusion.

Configurer le routage de multidiffusion Stub et transférer les messages IGMP



Remarque Le routage de multidiffusion de stub n'est pas pris en charge en même temps que les modes fragmenté et bidirectionnel de la PIM.

Un ASA agissant en tant que passerelle vers la zone de stub n'a pas besoin de participer au mode fractionné (PIM) ou au mode bidirectionnel. Au lieu de cela, vous pouvez le configurer pour qu'il agisse comme un agent mandataire et transfère les messages IGMP des hôtes connectés sur une interface vers un routeur de multidiffusion en amont sur une autre interface. Pour configurer l'ASA en tant qu'agent de mandataire IGMP, transférez les messages de jonction et de sortie de l'hôte de l'interface de zone de stub vers une interface en amont. Vous devez également activer la PIM sur les interfaces qui participent au routage de multidiffusion en mode stub.

Procédure

Configurez le routage de multidiffusion de stub et transférez les messages IGMP :

igmp forward interface if_name

Exemple :

```
ciscoasa(config-if)# igmp forward interface interface1
```

Configurer une route de multidiffusion statique

La configuration de routes statiques de multidiffusion vous permet de séparer le trafic de multidiffusion du trafic de monodiffusion. Par exemple, quand un chemin entre une source et une destination ne prend pas en charge le routage de multidiffusion, la solution consiste à configurer deux périphériques de multidiffusion avec un tunnel GRE et d'envoyer les paquets en multidiffusion sur le tunnel.

Lors de l'utilisation de PIM, l'ASA s'attend à recevoir des paquets sur la même interface où il renvoie les paquets de monodiffusion à la source. Dans certains cas, par exemple pour contourner une voie de routage

qui ne prend pas en charge le routage de multidiffusion, vous pouvez souhaiter que les paquets monodiffusion prennent un chemin et les paquets multidiffusion, un autre.

Les routes de multidiffusion statiques ne sont pas annoncées ou redistribuées.

Procédure

Étape 1 Configurez une route de multidiffusion statique :

mroute src_ip src_mask {input_if_name | *rpf_neighbor*} [distance]

Exemple :

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
```

Étape 2 Configurez une route de multidiffusion statique pour une zone de stub :

mroute src_ip src_mask input_if_name [**dense** output_if_name] [distance]

Exemple :

```
ciscoasa(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]
```

Le paire mot clé-argument **dense** *output_if_name* n'est prise en charge que pour le routage de multidiffusion de stub.

Configurer des fonctionnalités IGMP

Les hôtes IP utilisent le protocole IGMP pour signaler leur appartenance à des groupes aux routeurs de multidiffusion connectés directement. IGMP est utilisé pour enregistrer dynamiquement des hôtes individuels dans un groupe de multidiffusion sur un réseau local particulier. Les hôtes déterminent les appartenances aux groupes en envoyant des messages IGMP à leur routeur de multidiffusion local. Sous IGMP, les routeurs écoutent les messages IGMP et envoient périodiquement des requêtes pour découvrir quels groupes sont actifs ou inactifs sur un sous-réseau particulier.

Cette section décrit comment configurer les paramètres IGMP facultatifs pour l'interface.

Désactiver IGMP sur une interface

Vous pouvez désactiver IGMP sur des interfaces spécifiques. Cela est utile si vous savez qu'il n'y a aucun hôte en multidiffusion sur une interface spécifique et que vous souhaitez empêcher l'ASA d'envoyer des messages de requête d'hôte sur cette interface.

Procédure

Désactivez IGMP sur une interface :

no igmp

Exemple :

```
ciscoasa(config-if)# no igmp
```

Pour réactiver IGMP sur une interface, utilisez la commande **igmp**.

Remarque
Seule la commande **no igmp** apparaît dans la configuration d'interface.

Configurer l'appartenance au groupe IGMP

Vous pouvez configurer l'ASA pour qu'il soit membre d'un groupe de multidiffusion. La configuration de l'ASA pour se joindre à un groupe de multidiffusion fait en sorte que les routeurs en amont conservent les renseignements de la table de routage de multidiffusion pour ce groupe et maintiennent les chemins de ce groupe actifs.

Remarque Si vous souhaitez transférer des paquets en multidiffusion pour un groupe spécifique vers une interface sans que l'ASA n'accepte ces paquets dans le cadre du groupe, consultez Configurer un groupe IGMP joint statiquement, à la page 1188.

Procédure

Configurez l'ASA pour qu'il soit membre d'un groupe de multidiffusion :

igmp join-group group-address

Exemple :

```
ciscoasa(config-if)# igmp join-group mcast-group
```

L'argument *group-address* est l'adresse IP du groupe.

Remarque
La commande **igmp join-group** permet à PIM d'envoyer des demandes de *jonction* vers les sources ou vers le point de rendez-vous (RP), à condition que le pare-feu avec cette commande soit le routeur désigné PIM (DR) sur l'interface où la commande est appliquée.

Configurer un groupe IGMP joint statiquement

Parfois, un membre d'un groupe ne peut pas signaler son appartenance au groupe en raison d'une configuration, ou il se peut qu'il n'y ait aucun membre d'un groupe sur le segment de réseau. Cependant, vous souhaitez toujours que le trafic de multidiffusion de ce groupe soit envoyé vers ce segment de réseau. Vous pouvez envoyer le trafic de multidiffusion pour ce groupe au segment en configurant un groupe IGMP rejoint statiquement.

Entrez la commande **igmp static-group**. L'ASA n'accepte pas les paquets de multidiffusion, mais les transfère plutôt vers l'interface spécifiée.

Procédure

Configurez l'ASA de manière statique pour qu'il rejoigne un groupe de multidiffusion sur une interface :

igmp static-group

Exemple :

```
ciscoasa(config-if)# igmp static-group group-address
```

L'argument *group-address* est l'adresse IP du groupe.

Remarque
La commande **igmp static-group** permet à PIM d'envoyer des demandes de *jonction* vers les sources ou vers le point de rendez-vous (RP), à condition que le pare-feu avec cette commande soit le routeur désigné PIM (DR) sur l'interface où la commande est appliquée.

Contrôler l'accès aux groupes de multidiffusion

Vous pouvez contrôler l'accès aux groupes de multidiffusion à l'aide de listes de contrôle d'accès.

Procédure

Étape 1 Créez une ACL standard pour le trafic de multidiffusion :

access-list name **standard** [**permit | deny]** ip_addr mask

Exemple :

```
ciscoasa(config)# access-list acl1 standard permit 192.52.662.25
```

Vous pouvez créer plusieurs entrées pour une seule ACL. Vous pouvez utiliser des ACL étendues ou standard.

L'argument *ip_addr mask* est l'adresse IP du groupe de multidiffusion qui est autorisée ou refusée.

Étape 2 Créez une ACL étendue :

access-list name **extended** [**permit | deny]** protocol src_ip_addr src_mask dst_ip_addr dst_mask

Exemple :

```
ciscoasa(config)# access-list acl2 extended permit protocol
src_ip_addr src_mask dst_ip_addr dst_mask
```

L'argument *dst_ip_addr* est l'adresse IP du groupe de multidiffusion qui est autorisée ou refusée.

Étape 3 Appliquez l'ACL à une interface :

igmp access-group acl

Exemple :

```
ciscoasa(config-if)# igmp access-group acl
```

L'argument *acl* est le nom d'une ACL IP standard ou étendue.

Limiter le nombre d'états IGMP sur une interface

Vous pouvez limiter le nombre d'états IGMP résultant des rapports sur les membres IGMP pour chaque interface. Les rapports sur les membres dépassant les limites configurées ne sont pas entrés dans la mémoire cache IGMP et le trafic pour les rapports sur les membres excédentaires n'est pas transféré.

Procédure

Limitez le nombre d'états IGMP sur une interface :

igmp limit number

Exemple :

```
ciscoasa(config-if)# igmp limit 50
```

Les valeurs valides sont comprises entre 0 et 5 000, étant la valeur par défaut.

La définition de cette valeur à 0 empêche l'ajout de groupes appris, mais les appartenances définies manuellement (à l'aide des commandes **igmp join-group** et **igmp static-group**) sont toujours autorisées. La forme **no** (non) de cette commande rétablit la valeur par défaut.

Remarque Lorsque vous modifiez la limite IGMP sur l'interface avec des jonctions actives, la nouvelle limite ne s'applique pas aux groupes existants. L'ASA valide la limite uniquement lorsqu'un nouveau groupe est ajouté à l'interface ou lorsque les minuteries de jonction IGMP expirent. Pour appliquer la nouvelle limite avec effet immédiat, vous devez désactiver et réactiver IGMP sur l'interface.

Modifier les messages de requête destinés aux groupes de multidiffusion

L'ASA envoie des messages de requête pour découvrir quels groupes de multidiffusion ont des membres sur les réseaux connectés aux interfaces. Les membres répondent par des messages de rapport IGMP indiquant qu'ils souhaitent recevoir des paquets en multidiffusion pour des groupes spécifiques. Les messages de requête sont adressés au groupe de multidiffusion tous les systèmes, qui possède l'adresse 224.0.0.1 et une valeur de durée de vie de 1.

Ces messages sont envoyés périodiquement pour actualiser les renseignements sur les membres stockés sur l'ASA. Si l'ASA découvre qu'il n'y a aucun membre local d'un groupe de multidiffusion connecté à une interface, il arrête de transférer le paquet en multidiffusion pour ce groupe vers le réseau connecté et il renvoie un message d'élaguer à la source des paquets.

Par défaut, le routeur désigné PIM sur le sous-réseau est responsable de l'envoi des messages de requête. Par défaut, ils sont envoyés toutes les 125 secondes.

Lors de la modification du temps de réponse aux requêtes, par défaut, le temps de réponse maximal aux requêtes annoncé dans les requêtes IGMP est de 10 secondes. Si l'ASA ne reçoit pas de réponse à une requête d'hôte dans ce délai, il supprime le groupe.



Remarque Les commandes **igmp query-timeout** et **igmp query-interval** nécessitent IGMP version 2.

Pour modifier l'intervalle de requête, le temps de réponse à la requête et la valeur du délai d'expiration de la requête, procédez comme suit :

Procédure

Étape 1 Définissez la durée de l'intervalle de requête en secondes :

igmp query-interval *seconds*

Exemple :

```
ciscoasa(config-if)# igmp query-interval 30
```

Les valeurs valides vont de 1 à 3600; la valeur par défaut est 125.

Si l'ASA n'entend pas de message de requête sur une interface pendant le délai d'expiration spécifié (255 secondes par défaut), l'ASA devient le routeur désigné et commence à envoyer les messages de requête.

Étape 2 Modifiez la valeur du délai d'expiration de la requête :

igmp query-timeout *seconds*

Exemple :

```
ciscoasa(config-if)# igmp query-timeout 30
```

Les valeurs valides vont de 60 à 300; la valeur par défaut est 225.

Étape 3 Modifiez le temps de réponse maximum aux requêtes :

igmp query-max-response-time *seconds*

Les valeurs valides vont de 1 à 25; la valeur par défaut est 10.

Exemple :

```
ciscoasa(config-if)# igmp query-max-response-time 20
```

Modifier la version IGMP

Par défaut, l'ASA exécute la version 2 du protocole IGMP, qui active plusieurs fonctionnalités supplémentaires telles que les commandes **igmp query-timeout** et **igmp query-interval** .

Tous les routeurs de multidiffusion d'un sous-réseau doivent prendre en charge la même version d'IGMP. L'ASA ne détecte pas automatiquement les routeurs de la version 1 et passe à la version 1. Cependant, une combinaison d'hôtes IGMP versions 1 et 2 sur le sous-réseau fonctionne; l'ASA exécutant IGMP version 2 fonctionne correctement lorsque des hôtes IGMP version 1 sont présents.

Procédure

Contrôlez la version d'IGMP que vous souhaitez exécuter sur l'interface :

igmp version {**1** | **2**}

Exemple :

```
ciscoasa(config-if)# igmp version 2
```

Configurer des fonctionnalités PIM

Les routeurs utilisent PIM pour gérer les tableaux de transfert à utiliser pour le transfert des diagrammes de multidiffusion. Lorsque vous activez le routage de multidiffusion sur ASA, PIM et IGMP sont automatiquement activés sur toutes les interfaces.



Remarque Le protocole PIM n'est pas pris en charge avec PAT. Le protocole PIM n'utilise pas de ports et PAT ne fonctionne qu'avec les protocoles qui utilisent des ports.

Cette section décrit comment configurer les paramètres PIM optionnels.

Activer et désactiver la PIM sur une interface

Vous pouvez activer ou désactiver la PIM sur des interfaces spécifiques.

Procédure

Étape 1 Activez ou réactivez la PIM sur une interface spécifique :

pim

Exemple :

```
ciscoasa(config-if)# pim
```

Étape 2 Désactivez la PIM sur une interface spécifique :

no pim

Exemple :

```
ciscoasa(config-if)# no pim
```

Remarque
Seule la commande **no pim** apparaît dans la configuration d'interface.

Configurer une adresse de point de rendez-vous statique

Tous les routeurs d'un mode PIM fragmenté ou d'un domaine bidirectionnel commun doivent connaître l'adresse PRV PIM. L'adresse est configurée de manière statique à l'aide de la commande **pim rp-address**.

Remarque L'ASA ne prend pas en charge le PRV automatique. Vous devez utiliser la commande **pim rp-address** pour spécifier l'adresse PRV.

Vous pouvez configurer l'ASA pour qu'il serve de PRV à plus d'un groupe. La plage de groupes spécifiée dans la liste de contrôle d'accès détermine le mappage du groupe RP PIM. Si aucune ACL n'est précisée, le RP du groupe est appliqué à l'ensemble de la plage du groupe de multidiffusion (224.0.0.0/4).

Procédure

Activez ou réactivez la PIM sur une interface spécifique :

pim rp-address ip_address [acl] [**bidir**]

L'argument *ip_address* est l'adresse IP de monodiffusion du routeur attribué comme PRV PIM.

L'argument *acl* est le nom ou le numéro d'une ACL standard qui définit avec quels groupes de multidiffusion le PRV doit être utilisé. N'utilisez pas une ACL d'hôte avec cette commande.

L'exclusion du mot clé **bidir** fait que les groupes fonctionnent en mode PIM fragmenté.

Remarque
L'ASA annonce toujours la capacité bidirectionnelle dans les messages Hello de PIM, quelle que soit la configuration bidirectionnel réelle.

Exemple :

```
ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]
```

Configurer la priorité des routeurs désignés

Le DR est responsable de l'envoi des messages PIM de registre, de jonction et de suppression au RP. Lorsqu'il y a plusieurs routeurs de multidiffusion sur un segment de réseau, la sélection du DR se fait en fonction de la priorité DR. Si plusieurs périphériques ont le même DR, le périphérique avec l'adresse IP la plus élevée devient DR.

Par défaut, l'ASA a une priorité DR de 1. Vous pouvez modifier cette valeur.

Procédure

Changez la priorité du routeur désigné :

pim dr-priority num

Exemple :

```
ciscoasa(config-if)# pim dr-priority 500
```

L'argument *num* peut être n'importe quel nombre compris entre 1 et 4294967294.

Configurer et filtrer les messages de registre PIM

Lorsque l'ASA agit comme un PRV, vous pouvez empêcher certaines sources en multidiffusion de s'enregistrer auprès de lui pour empêcher les sources non autorisées de s'enregistrer auprès du PRV. Le volet Request Filter (Filtre de demande) vous permet de définir les sources en multidiffusion dont l'ASA accepte les messages de registre PIM.

Procédure

Configurez l'ASA pour filtrer les messages de registre PIM :

pim accept-register {**list** acl | **route-map** map-name}

Exemple :

```
ciscoasa(config)# pim accept-register {list acl1 | route-map map2}
```

Dans l'exemple, l'ASA filtre les messages de registre PIM *acl1* et de carte de routage *map2*.

Configurer les intervalles des messages PIM

Les messages de requête de routeur sont utilisés pour sélectionner le PIM DR. Le PIM DR est responsable de l'envoi des messages d'interrogation du routeur. Par défaut, des messages de requête du routeur sont envoyés toutes les 30 secondes. En outre, toutes les 60 secondes, l'ASA envoie des messages de jonction ou d'élimination PIM.

Procédure

Étape 1 Envoyez les messages de requête du routeur :

pim hello-interval seconds

Exemple :

```
ciscoasa(config-if)# pim hello-interval 60
```

Les valeurs valides pour l'argument *seconds* sont comprises entre 1 et 3 600 secondes.

Étape 2 Modifiez la durée (en secondes) pendant laquelle l'ASA envoie des messages de jonction ou d'élimination PIM :

pim join-prune-interval seconds

Exemple :

```
ciscoasa(config-if)# pim join-prune-interval 60
```

Les valeurs valides pour l'argument *seconds* sont comprises entre 10 et 600 secondes.

Filtrer les voisins PIM

Vous pouvez définir les routeurs qui peuvent devenir des voisins PIM. En filtrant les routeurs qui peuvent devenir des voisins PIM, vous pouvez effectuer les opérations suivantes :

- Empêchez les routeurs non autorisés de devenir des voisins PIM.
- Empêchez les routeurs tampons connectés de participer à PIM.

Procédure

Étape 1 Utilisez une ACL standard pour définir les routeurs que vous souhaitez voir participer à la PIM :

access-list pim_nbr deny *router-IP_addr PIM neighbor*

Exemple :

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

Dans l'exemple, l'ACL suivante, lorsqu'elle est utilisée avec la commande **pim neighbor-filter**, empêche le routeur 10.1.1.1 de devenir un voisin PIM.

Étape 2 Filtrez les routeurs voisins :

pim neighbor-filter pim_nbr

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim neighbor-filter pim_nbr
```

Dans l'exemple, le routeur 10.1.1.1 ne peut pas devenir un voisin PIM sur l'interface GigabitEthernet0/3.

Configurer un filtre de voisin bidirectionnel PIM

Le volet Bidirectional Neighbor Filter (Filtre de voisin bidirectionnel) affiche les filtres de voisin bidirectionnel de la PIM, le cas échéant, qui sont configurés sur l'ASA. Un filtre de voisin bidirectionnel PIM est une ACL qui définit les périphériques voisins pouvant participer au choix du DF. Si un filtre de voisin bidirectionnel PIM n'est pas configuré pour une interface, il n'y a aucune restriction. Si un filtre de voisin bidirectionnel PIM est configuré, seuls les voisins autorisés par la liste de contrôle d'accès peuvent participer au processus de sélection de DF.

Lorsqu'une configuration de filtre de voisin bidirectionnel PIM est appliquée à l'ASA, une ACL s'affiche dans la configuration en cours d'exécution avec le nom *interface-name_multicast*, dans lequel le *interface-name* est le nom de l'interface à laquelle le filtre de limite de multidiffusion est appliqué. Si une ACL porte déjà ce nom, un numéro est affecté au nom (par exemple, inside_multicast_1). Cette ACL définit quels appareils peuvent devenir des voisins PIM de l'ASA.

Le PIM bidirectionnel permet aux routeurs de multidiffusion de conserver des informations d'état réduites. Tous les routeurs de multidiffusion d'un segment doivent être activés de manière bidirectionnelle pour choisir un DF.

Les filtres de voisin bidirectionnels de la PIM permettent la transition d'un réseau en mode fragmenté uniquement vers un réseau bidirectionnel en vous permettant de spécifier les routeurs qui doivent participer au choix du DF, tout en permettant à tous les routeurs de participer au domaine en mode fragmenté. Les routeurs bidirectionnels peuvent choisir un DF entre eux, même s'il y a des routeurs non-bidirectionnels sur le segment. La multidiffusion sur les routeurs non-bidirectionnels empêche les messages PIM et les données des groupes bidirectionnels de fuir vers l'intérieur ou l'extérieur du sous-ensemble bidirectionnel.

Lorsqu'un filtre de voisin bidirectionnel PIM est activé, les routeurs autorisés par la liste de contrôle d'accès sont considérés comme bidirectionnels. Par conséquent, ce qui suit est vrai :

- Si un voisin autorisé ne prend pas en charge le mode bidirectionnel, le choix du DF n'a pas lieu.
- Si un voisin refusé prend en charge le mode bidirectionnel, le choix du DF n'a pas lieu.
- Si un voisin refusé ne prend pas en charge le mode bidirectionnel, le choix du DF peut avoir lieu.

Procédure

Étape 1 Utilisez une ACL standard pour définir les routeurs que vous souhaitez voir participer à la PIM :

access-list pim_nbr deny *router-IP_addr PIM neighbor*

Exemple :

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

Dans l'exemple, l'ACL suivante, lorsqu'elle est utilisée avec la commande **pim neighbor-filter**, empêche le routeur 10.1.1.1 de devenir un voisin PIM.

Étape 2 Filtrez les routeurs voisins :

pim bidirectional-neighbor-filter pim_nbr

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr
```

Dans l'exemple, le routeur 10.1.1.1 ne peut pas devenir un voisin bidirectionnel PIM sur l'interface GigabitEthernet0/3.

Configurer l'ASA comme candidat BSR

Vous pouvez configurer l'ASA en tant que BSR candidat.

Procédure

Étape 1 Configurez le routeur pour qu'il annonce sa candidature en tant que routeur de démarrage (BSR) :

pim bsr-candidate *interface_name* [*hash_mask_length* [*priority*]]

Exemple :

```
ciscoasa(config)# pim bsr-candidate inside 12 3
```

Étape 2 (Facultatif) Configurez l'ASA en tant que routeur de démarrage frontalier :

interface *interface_name*

pim bsr-border

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# pim bsr-border
```

Lorsque cette commande est configurée sur une interface, aucun message de routeur de démarrage (BSR) ne sera envoyé ou reçu par le biais d'une interface.

Configurer une limite de multidiffusion

La portée des adresses définit des limites de domaine afin que les domaines dont les RP ont la même adresse IP n'empiètent pas l'un sur l'autre. La détermination de la portée est effectuée sur les limites du sous-réseau au sein des grands domaines et sur les limites entre le domaine et Internet.

Vous pouvez configurer une limite de portée administrative sur une interface pour les adresses de groupe de multidiffusion. L'IANA a désigné la plage d'adresses en multidiffusion de 239.0.0.0 à 239.255.255.255 comme adresses de portée administrative. Cette plage d'adresses peut être réutilisée dans des domaines administrés par différentes organisations. Les adresses seraient considérées comme locales et non uniques mondialement.

Une liste de contrôle d'accès standard définit la plage d'adresses concernées. Lorsqu'une limite est configurée, aucun paquet de données en multidiffusion ne peut traverser la limite dans aucune direction. La limite permet à la même adresse de groupe de multidiffusion d'être réutilisée dans différents domaines administratifs.

Vous pouvez configurer, examiner et filtrer les messages de découverte et d'annonce Auto-RP à la limite administrative en saisissant le mot clé **filter-autorp**. Toutes les annonces de plage de groupes Auto-RP des paquets Auto-RP qui sont refusées par l'ACL de frontière sont supprimées. Une annonce de plage de groupes Auto-RP est autorisée et transmise par la limite uniquement si toutes les adresses de la plage de groupes Auto-RP sont autorisées par la liste de contrôle d'accès (ACL) de limite. Si une adresse n'est pas autorisée, la plage complète de groupe est filtrée et supprimée du message Auto-RP avant que le message Auto-RP ne soit transféré.

Procédure

Configurez une limite de multidiffusion :

multicast boundary acl [**filter-autorp**]

Exemple :

```
ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]
```

Supervision de PIM

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage PIM. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande.

Pour superviser ou désactiver diverses statistiques de routage PIM, saisissez l'une des commandes suivantes :

- **show pim bsr-router**

  Affiche les renseignements sur le routeur de démarrage.

- **show mroute**

  Affiche le contenu de la table de routage multidiffusion.

- **show mfib summary**

Affiche des renseignements récapitulatifs sur le nombre d'entrées et d'interfaces de la base d'information de transfert multidiffusion PIM IPv4.

- **show mfib active**

  Affiche les renseignements de la base d'information de transfert multidiffusion (MFIB) sur le débit auquel les sources de multidiffusion actives envoient des données aux groupes de multidiffusion.

- **show pim group-map**

  Affiche le mappage de groupe vers le mode PIM. Pour afficher le RP choisi pour un groupe, précisez l'adresse ou le nom du groupe.

- **show pim group-map rp-timers**

  Affiche l'expiration et le temps de disponibilité de la minuterie pour chaque entrée de mappage de groupe vers le mode PIM.

- **show pim neighbor**

  Affiche les voisins PIM (Protocole Independent Multicast).

Exemple de routage de multidiffusion

L'exemple suivant montre comment activer et configurer le routage de multidiffusion à l'aide de différents processus facultatifs :

1. Activez le routage de multidiffusion :

```
ciscoasa(config)# multicast-routing
```

2. Configurez une route de multidiffusion statique :

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
ciscoasa(config)# exit
```

3. Configurez l'ASA pour qu'il soit membre d'un groupe de multidiffusion :

```
ciscoasa(config)# interface
ciscoasa(config-if)# igmp join-group group-address
```

Historique du routage de multidiffusion

Tableau 44 : Historique des fonctionnalités du routage de multidiffusion

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du routage de multidiffusion	7.0(1)	La prise en charge des données de routage de multidiffusion, de l'authentification, de la redistribution et de la surveillance des informations de routage à l'aide du protocole de routage de multidiffusion a été ajoutée. Nous avons introduit la commande **multicast-routing**.
Prise en charge de la mise en grappe	9.0(1)	Une prise en charge a été ajoutée pour la mise en grappe. Nous avons introduit les commandes suivantes : **debug mfib cluster**, **show mfib cluster**.
Prise en charge du protocole PIM (Protocol Independent Multicast) en multidiffusion propre à la source (PIM-SSM)	9.5(1)	Une prise en charge a été ajoutée pour permettre aux paquets PIM-SSM de transiter lorsque le routage de multidiffusion est activé, sauf si l'ASA est le routeur de dernier saut. Cela permet une plus grande flexibilité dans le choix d'un groupe de multidiffusion tout en vous assurant une protection contre différentes attaques; les hôtes ne reçoivent que le trafic de sources explicitement demandées. Nous n'avons pas modifié de commandes.
Routeur de démarrage PIM (Protocol Independent Multicast)	9.5(2)	Une prise en charge a été ajoutée pour un nouveau modèle de sélection dynamique des points de rendez-vous (PRV) qui utilise des routeurs candidats pour la fonction Point de rendez-vous et pour le relais des informations Point de rendez-vous pour un groupe. Cette fonctionnalité fournit un moyen d'apprendre dynamiquement les points de rendez-vous (PRV), ce qui est tout à fait essentiel dans les grands réseaux complexes où un PRV peut périodiquement tomber en panne et se relancer. Nous avons ajouté les commandes suivantes : clear pim group-map, debug pim bsr, pim bsr-border, pim bsr-candidate, show pim bsr-router, show pim group-map rp-timers
Limite igmp augmentée	9.15(1) *Également dans 9.12(4)*	La limite igmp a été augmentée de 500 à 5 000. Commandes nouvelles ou modifiées : **igmp limit**.



PARTIE VI

Serveurs AAA et base de données locale

- AAA et base de données locale, à la page 1203
- Serveurs RADIUS pour AAA, à la page 1215
- Serveurs TACACS+ pour AAA, à la page 1237
- Serveurs LDAP pour AAA, à la page 1245
- Serveurs Kerberos pour AAA, à la page 1259
- Configurer les serveurs RSA SecurID pour AAA, à la page 1267



CHAPITRE 37

AAA et base de données locale

Ce chapitre décrit l'authentification, l'autorisation et la traçabilité (AAA, prononcé « trois A »). Le protocole AAA regroupe un ensemble de services destinés à contrôler l'accès aux ressources informatiques, à appliquer des politiques, à évaluer l'utilisation et à fournir les renseignements nécessaires pour facturer les services. Ces processus sont considérés comme importants pour une gestion et une sécurité efficaces du réseau.

Ce chapitre décrit également comment configurer la base de données locale pour la fonctionnalité AAA. Pour les serveurs AAA externes, consultez le chapitre correspondant à votre type de serveur.

- À propos d'AAA et de la base de données locale, à la page 1203
- Lignes directrices relatives à la base de données locale, à la page 1208
- Ajouter un compte d'utilisateur à la base de données locale, à la page 1208
- Supervision de la base de données locale, à la page 1210
- Historique de la base de données locale, à la page 1211

À propos d'AAA et de la base de données locale

Cette section décrit AAA et la base de données locale.

Authentification

L'authentification fournit un moyen d'identifier un utilisateur, généralement en demandant à l'utilisateur de saisir un nom d'utilisateur et un mot de passe valides avant que l'accès ne soit accordé. Le serveur AAA compare les renseignements d'authentification d'un utilisateur à ceux d'autres utilisateurs stockés dans une base de données. Si les renseignements d'authentification correspondent, l'utilisateur est autorisé à accéder au réseau. Dans le cas contraire, l'authentification échoue et l'accès au réseau est refusé.

Vous pouvez configurer l'ASA pour authentifier les éléments suivants :

- Toutes les connexions administratives à l'ASA, y compris les sessions suivantes :
  - Telnet
  - SSH
  - Console de série
  - ASDM à l'aide de HTTPS
  - Accès à la gestion du VPN

- La commande **enable**
- Accès au réseau
- Accès VPN

Autorisation

L'autorisation est le processus d'application des politiques : qui détermine les types d'activités, de ressources ou de services auxquels un utilisateur est autorisé à accéder. Une fois qu'un utilisateur est authentifié, cet utilisateur peut être autorisé pour différents types d'accès ou d'activités.

Vous pouvez configurer l'ASA pour autoriser les éléments suivants :

- Commandes de gestion
- Accès au réseau
- Accès VPN

Comptabilité

La comptabilité mesure les ressources qu'un utilisateur consomme lors de l'accès, qui peuvent inclure la durée du système ou la quantité de données qu'un utilisateur a envoyées ou reçues au cours d'une session. La comptabilisation est effectuée au moyen de la journalisation des statistiques de session et des renseignements d'utilisation, qui sont utilisés pour les activités de contrôle des autorisations, de facturation, d'analyse des tendances, d'utilisation des ressources et de planification de la capacité.

Interaction entre authentification, autorisation et traçabilité

Vous pouvez utiliser l'authentification seule ou avec l'autorisation et la comptabilité. L'autorisation nécessite toujours qu'un utilisateur soit d'abord authentifié. Vous pouvez utiliser la comptabilité seule ou avec l'authentification et l'autorisation.

Serveurs et groupes de serveurs AAA

Le serveur AAA est un serveur de réseau utilisé pour le contrôle d'accès. L'authentification identifie l'utilisateur. L'autorisation met en œuvre des politiques qui déterminent les ressources et les services auxquels un utilisateur authentifié peut accéder. La comptabilité fait le suivi des ressources de temps et de données utilisées pour la facturation et l'analyse.

Si vous souhaitez utiliser un serveur AAA externe, vous devez d'abord créer un groupe de serveurs AAA pour le protocole utilisé par le serveur externe et ajouter le serveur au groupe. Vous pouvez créer plusieurs groupes par protocole et des groupes distincts pour tous les protocoles que vous souhaitez utiliser. Chaque groupe de serveurs est propre à un type de serveur ou de service.

Consultez les rubriques suivantes pour en savoir plus sur la création des groupes :

- Configurer les groupes de serveurs RADIUS, à la page 1229
- Configurer les groupes de serveurs TACACS+, à la page 1239
- Configurer les groupes de serveurs LDAP, à la page 1252

- Configurer les groupes de serveurs AAA Kerberos, à la page 1259
- Configurer les groupes de serveurs RSA SecurID pour AAA, à la page 1268

Consultez le guide de configuration de VPN pour en savoir plus sur l'utilisation de la délégation sous contraintes de Kerberos et du formulaire HTTP.

Le tableau suivant résume les types de serveurs pris en charge et leurs utilisations, y compris la base de données locale.

Tableau 45 : Services pris en charge pour les serveurs AAA

Type de serveur et service	Authentification	Autorisation	Gestion de comptes
Base de données locale			
Administrateurs	Oui	Oui	Non
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Oui	Oui	Non
RADIUS			
Administrateurs	Oui	Oui	Oui
Utilisateurs VPN	Oui	Oui	Oui
Sessions de pare-feu (règles AAA)	Oui	Oui	Oui
TACACS+			
Administrateurs	Oui	Oui	Oui
Utilisateurs VPN	Oui	Non	Oui
Sessions de pare-feu (règles AAA)	Oui	Oui	Oui
LDAP			
Administrateurs	Oui	Non	Non
Utilisateurs VPN	Oui	Oui	Non
Sessions de pare-feu (règles AAA)	Oui	Non	Non
Kerberos			
Administrateurs	Oui	Non	Non
Utilisateurs VPN	Oui	Non	Non

Type de serveur et service	Authentification	Autorisation	Gestion de comptes
Sessions de pare-feu (règles AAA)	Oui	Non	Non
SDI (RSA SecurID)			
Administrateurs	Oui	Non	Non
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Oui	Non	Non
Formulaire HTTP			
Administrateurs	Non	Non	Non
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Non	Non	Non

Notes

- RADIUS : la comptabilisation des administrateurs n'inclut pas la comptabilisation des commandes.
- RADIUS : l'autorisation des sessions de pare-feu est prise en charge uniquement avec les listes d'accès spécifiques à l'utilisateur, qui sont reçues ou spécifiées dans une réponse à la demande d'authentification RADIUS.
- TACACS+ : la comptabilisation des administrateurs comprend la comptabilisation des commandes.
- Formulaire HTTP : opérations d'authentification et SSO pour les sessions utilisateur du SSL VPN sans client uniquement.

À propos de la base de données locale

L'ASA gère une base de données locale que vous pouvez remplir avec les profils d'utilisateurs. Vous pouvez utiliser une base de données locale au lieu de serveurs AAA pour assurer l'authentification, l'autorisation et la traçabilité des utilisateurs.

Vous pouvez utiliser la base de données locale pour les fonctions suivantes :

- Accès à ASDM par utilisateur
- Authentification de la console
- Authentification Telnet et SSH
- Authentification de la commande **enable**

  Ce paramètre est réservé à l'accès à l'interface de ligne de commande et n'influe pas sur la connexion à Cisco ASDM.
- Autorisation de commande

Si vous activez l'autorisation de commande à l'aide de la base de données locale, l'ASA fait référence au niveau de privilège de l'utilisateur pour déterminer quelles commandes sont disponibles. Sinon, le niveau de privilège n'est généralement pas utilisé. Par défaut, toutes les commandes sont de niveau de privilège 0 ou de niveau 15.

- Authentification d'accès au réseau
- Authentification du client VPN

Pour le mode de contexte multiple, vous pouvez configurer les noms d'utilisateur dans l'espace d'exécution du système pour fournir des connexions individuelles au niveau de l'interface de ligne de commande à l'aide de la commande **login**; cependant, vous ne pouvez pas configurer de règles AAA qui utilisent la base de données locale dans l'espace d'exécution du système.



Remarque Vous ne pouvez pas utiliser la base de données locale pour l'autorisation d'accès au réseau.

Prise en charge du basculement

La base de données locale peut servir de méthode de secours pour plusieurs fonctions. Ce comportement est conçu pour vous aider à éviter le verrouillage accidentel de l'ASA.

Lorsqu'un utilisateur se connecte, les serveurs du groupe sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde. Si tous les serveurs du groupe sont indisponibles, l'ASA essaie la base de données locale si vous l'avez configurée comme méthode de secours (pour l'authentification et l'autorisation de gestion uniquement). Si vous n'avez pas de méthode de secours, l'ASA continue d'essayer les serveurs AAA.

Pour les utilisateurs qui ont besoin d'une prise en charge de secours, nous recommandons que leurs noms d'utilisateur et mots de passe dans la base de données locale correspondent à leurs noms d'utilisateur et mots de passe sur les serveurs AAA. Cette pratique offre une prise en charge de secours transparente. Étant donné que l'utilisateur ne peut pas déterminer si un serveur AAA ou la base de données locale fournit le service, l'utilisation de noms d'utilisateur et de mots de passe sur des serveurs AAA qui sont différents de ceux de la base de données locale signifie que l'utilisateur ne peut pas être certain du nom d'utilisateur et du mot de passe à fournir.

La base de données locale prend en charge les fonctions de secours suivantes :

- Console et activation de l'authentification par mot de passe : si les serveurs du groupe sont tous indisponibles, l'ASA utilise la base de données locale pour authentifier l'accès administratif, qui peut également inclure l'activation de l'authentification par mot de passe.
- Autorisation de commande : si les serveurs TACACS+ du groupe sont tous indisponibles, la base de données locale est utilisée pour autoriser les commandes en fonction des niveaux de privilège.
- Authentification et autorisation VPN : l'authentification et l'autorisation VPN sont prises en charge pour permettre l'accès à distance à l'ASA si les serveurs AAA qui prennent normalement en charge ces services VPN ne sont pas disponibles. Lorsqu'un client VPN d'un administrateur spécifie un groupe de tunnels configuré pour un basculement vers la base de données locale, le tunnel VPN peut être établi même si le groupe de serveurs AAA n'est pas disponible, à condition que la base de données locale soit configurée avec les attributs nécessaires.

Fonctionnement du basculement avec plusieurs serveurs dans un groupe

Si vous configurez plusieurs serveurs dans un groupe de serveurs et que vous activez le basculement vers la base de données locale pour le groupe de serveurs, le basculement se produit lorsqu'aucun serveur du groupe ne répond à la demande d'authentification de l'ASA. Par exemple, envisagez le scénario suivant :

Vous configurez un groupe de serveurs LDAP avec deux serveurs Active Directory, le serveur 1 et le serveur 2, dans cet ordre. Lorsque l'utilisateur distant se connecte, l'ASA tente de s'authentifier auprès du serveur 1.

Si le serveur 1 répond par un échec d'authentification (par exemple, un utilisateur introuvable), l'ASA ne tente pas de s'authentifier auprès du serveur 2.

Si le serveur 1 ne répond pas dans le délai d'expiration (ou si le nombre de tentatives d'authentification dépasse le maximum configuré), l'ASA essaie le serveur 2.

Si les deux serveurs du groupe ne répondent pas et que l'ASA est configuré pour revenir à la base de données locale, l'ASA tente de s'authentifier auprès de la base de données locale.



Remarque Par défaut, un client RADIUS envoie trois demandes avant d'expirer. Lorsque le client tente d'établir une connexion SSH, la demande est envoyée à un serveur à la fois. À l'expiration des demandes, le serveur est marqué comme ayant ÉCHOUÉ. La prochaine demande RADIUS est envoyée au serveur ACTIF suivant, marquant par la suite tous les serveurs comme ayant ÉCHOUÉ et revenant finalement à l'authentification LOCALE (si elle est configurée). Les serveurs marqués comme ayant ÉCHOUÉ finissent par se rétablir et sont rendus ACTIFS. Dans ce cas, si vous avez 3 ou 4 serveurs dans le groupe, vous pourriez observer des problèmes de connexion intermittents.

Lignes directrices relatives à la base de données locale

Assurez-vous d'empêcher un verrouillage de l'ASA lorsque vous utilisez la base de données locale pour l'authentification ou l'autorisation.

Ajouter un compte d'utilisateur à la base de données locale

Pour ajouter un utilisateur à la base de données locale, procédez comme suit :

Procédure

Étape 1 Créez un compte utilisateur.

username *username* [**password** *password*] [**privilege** *priv_level*]

Exemple :

```
ciscoasa(config)# username exampleuser1 password madmaxfuryroadrules privilege 1
```

Le mot clé**username** *username* est une chaîne de 3 à 64 caractères, utilisant n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), à l'exception des espaces et du point d'interrogation. Le

mot clé **password** *password* est une chaîne de 8 à 127 caractères. Il peut s'agir de n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), avec les exceptions suivantes :

- Aucun espace
- Aucun point d'interrogation
- Il est interdit d'utiliser trois caractères ASCII (ou plus) qui se suivent ou qui se répètent. Par exemple, les mots de passe suivants seront refusés :
  - **abc**utilisateur1
  - utilisateur**543**
  - utilisateur**aaaa**
  - utilisateur2**666**

Par exemple, vous souhaiterez peut-être créer un nom d'utilisateur sans mot de passe si vous utilisez l'authentification par clé publique SSH. Le mot clé **privilege** *priv_level* définit le niveau de privilège, qui varie de 0 à 15. La valeur par défaut est 2. Ce niveau de privilège est utilisé avec l'autorisation de commande.

Mise en garde
Si vous n'utilisez pas l'autorisation de commande (la commande **aaa authorization console LOCAL**), le niveau par défaut 2 permet l'accès de gestion au mode d'exécution privilégié. Si vous souhaitez limiter l'accès au mode d'exécution privilégié, définissez le niveau de privilège à 0 ou 1, ou utilisez la commande **service-type**.

Ces options moins utilisées ne s'affichent pas dans la syntaxe ci-dessus : le mot clé **nopassword** crée un compte d'utilisateur qui accepte n'importe quel mot de passe; cette option n'est pas sécurisée et n'est pas conseillée.

Le mot clé **encrypted** (pour les mots de passe de 32 caractères ou moins dans les versions 9.6 et antérieures) ou le mot clé **pbkdf2** (pour les mots de passe de plus de 32 caractères dans les versions 9.6 et ultérieures, et les mots de passe de toutes les longueurs dans les versions 9.7 et ultérieures) indique que le mot de passe est chiffré (à l'aide d'un hachage basé sur MD5 ou d'un hachage PBCDF2 (Password-Based Key Derivation Function 2)). Notez que les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Lorsque vous définissez un mot de passe dans la commande **username**, l'ASA le chiffre avant de l'enregistrer dans la configuration à des fins de sécurité. Lorsque vous entrez la commande **show running-config**, la commande **username** n'affiche pas le mot de passe réel. Elle affiche le mot de passe chiffré suivi du mot clé **encrypted** ou **pbkdf2**. Par exemple, si vous entrez le mot de passe « test », la sortie de la commande **show running-config** se présentera comme suit :

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

Vous ne saisirez le mot clé **encrypted** ou **pbkdf2** dans l'interface de ligne de commande que si vous coupez-collez un fichier de configuration pour l'utiliser dans un autre ASA et que vous utilisez le même mot de passe.

Étape 2 (Facultatif) Configurez les attributs de nom d'utilisateur.

username *nom d'utilisateur* **attributes**

Exemple :

```
ciscoasa(config)# username exampleuser1 attributes
```

L'argument *username* est le nom d'utilisateur que vous avez créé à la première étape.

Par défaut, les utilisateurs VPN que vous ajoutez avec cette commande n'ont aucun attribut ni association de stratégie de groupe. Vous devez configurer toutes les valeurs explicitement à l'aide de la commande **username attributes**. Consultez le guide de configuration de VPN pour en savoir plus.

Étape 3 (Facultatif) Configurez le niveau d'utilisateur si vous avez configuré l'autorisation de gestion à l'aide de la commande **aaa authorization exec**.

service-type {**admin** | **nas-prompt** | **remote-access**}

Exemple :

```
ciscoasa(config-username)# service-type admin
```

Le mot clé **admin** permet un accès complet à tous les services spécifiés par les commandes **aaa authentication console LOCAL**. Le mot clé **admin** est la valeur par défaut.

Le mot clé **nas-prompt** permet l'accès à l'interface de ligne de commande lorsque vous configurez la commande **aaa authentication** {**telnet** | **ssh** | **serial**} **console**, mais refuse l'accès à la configuration ASDM si vous configurez la commande **aaa authentication http console**. L'accès à la surveillance ASDM est autorisé. Si vous activez l'authentification avec la commande **aaa authentication enable console**, l'utilisateur ne peut pas accéder au mode d'exécution privilégié à l'aide de la commande **enable** (ou de la commande **login**).

Le mot clé **remote-access** refuse l'accès de gestion. Vous ne pouvez pas utiliser les services spécifiés par les commandes **aaa authentication console** (à l'exception du mot clé **serial**, l'accès série est autorisé).

Étape 4 (Facultatif) Pour l'authentification par clé publique des connexions SSH à l'ASA par utilisateur, consultez Configurer SSH pour l'accès par clé publique, à la page 1280.

Étape 5 (Facultatif) Si vous utilisez ce nom d'utilisateur pour l'authentification VPN, vous pouvez configurer de nombreux attributs VPN pour l'utilisateur. Consultez le guide de configuration de VPN pour en savoir plus.

Exemples

L'exemple suivant attribue un niveau de privilège de 15 au compte d'utilisateur admin :

```
ciscoasa(config)# username admin password farscape1 privilege 15
```

L'exemple suivant active l'autorisation de gestion, crée un compte d'utilisateur avec un mot de passe, passe en mode de configuration du nom d'utilisateur et spécifie un **service-type** de **nas-prompt** :

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOrgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

Supervision de la base de données locale

Consultez les commandes suivantes pour superviser la base de données locale :

- **show aaa-server**

  Cette commande affiche les statistiques de la base de données configurée. Pour effacer les statistiques du serveur AAA, saisissez la commande **clear aaa-server statistics**.

- **show running-config aaa-server**

  Cette commande montre la configuration en cours d'exécution du serveur AAA. Pour effacer la configuration du serveur AAA, saisissez la commande **clear configure aaa-server**.

Historique de la base de données locale

Tableau 46 : Historique de la base de données locale

Nom de la caractéristique	Versions de plateforme	Description
Configuration de la base de données locale pour AAA	7.0(1)	Décrit comment configurer la base de données locale pour une utilisation AAA. Nous avons introduit les commandes suivantes : **username**, **aaa authorization exec authentication-server**, **aaa authentication console LOCAL**, **aaa authorization exec LOCAL**, **service-type, aaa authentication** {**telnet | ssh | serial**} **console LOCAL**, **aaa authentication http console LOCAL**, **aaa authentication enable console LOCAL**, **show running-config aaa-server**, **show aaa-server**, **clear configure aaa-server**, **clear aaa-server statistics**.
Prise en charge de l'authentification par clé publique SSH	9.1(2)	Vous pouvez désormais activer l'authentification par clé publique pour les connexions SSH à l'ASA par utilisateur. Vous pouvez spécifier une clé formatée de fichier de clé publique (PKF) ou une clé Base64. La clé PKF peut comporter jusqu'à 4 096 bits. Utilisez le format PKF pour les clés qui sont trop grandes pour la prise en charge ASA du format Base64 (jusqu'à 2 048 bits). Nous avons introduit les commandes suivantes : **ssh authentication**. *Également disponible dans 8.4(4.1); la prise en charge du format de clé PKF uniquement dans 9.1(2).*

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de mots de passe plus longs pour les mots de passe locaux **username** et **enable** (jusqu'à 127 caractères)	9.6(1)	Vous pouvez désormais créer des mots de passe **username** et **enable** locaux jusqu'à 127 caractères (l'ancienne limite était de 32). Lorsque vous créez un mot de passe de plus de 32 caractères, il est stocké dans la configuration à l'aide d'un hachage PBCDF2 (Password-Based Key Derivation Function 2). Les mots de passe plus courts continuent d'utiliser la méthode de hachage basée sur MD5. Nous avons modifié les commandes suivantes : **enable, username**
Améliorations de l'authentification par clé publique SSH	9.6(2)	Dans les versions antérieures, vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer également l'authentification SSH AAA avec la base de données d'utilisateurs locale (**aaa authentication ssh console LOCAL**). La configuration est désormais modifiée de manière à ce que vous deviez explicitement activer l'authentification SSH AAA. Pour empêcher les utilisateurs d'utiliser un mot de passe au lieu de la clé privée, vous pouvez désormais créer un nom d'utilisateur sans mot de passe défini. Nous avons modifié les commandes suivantes : **ssh authentication, username**
Hachage PBKDF2 pour tous les mots de passe locaux **username** et **enable**	9.7(1)	Les mots de passe locaux **username** et **enable** de toutes les longueurs sont stockés dans la configuration à l'aide du hachage PBKDF2 (Password-Based Key Derivation Function 2). Auparavant, les mots de passe de 32 caractères et moins utilisaient la méthode de hachage basée sur MD5. Les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Consultez le chapitre « Logiciels et configurations » du Guide de configuration des opérations générales pour connaître les lignes directrices relatives à la rétrogradation. Nous avons modifié les commandes suivantes : **enable, username**

Nom de la caractéristique	Versions de plateforme	Description
Authentification distincte pour les utilisateurs disposant d'une authentification par clé publique SSH et les utilisateurs disposant de mots de passe	9.6(3)/9.8(1)	Dans les versions antérieures à 9.6(2), vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer explicitement l'authentification SSH AAA avec la base de données des utilisateurs locale (**aaa authentication ssh console LOCAL**). Dans 9.6(2), l'ASA vous a demandé d'activer explicitement l'authentification SSH AAA. Dans cette version, vous n'avez plus à activer explicitement l'authentification SSH AAA; lorsque vous configurez la commande **ssh authentication** pour un utilisateur, l'authentification locale est activée par défaut pour les utilisateurs avec ce type d'authentification. De plus, lorsque vous configurez explicitement l'authentification SSH AAA, cette configuration s'applique uniquement aux noms d'utilisateur avec *mots de passe*, et vous pouvez utiliser n'importe quel type de serveur AAA (**aaa authentication ssh console radius_1**, par exemple). Par exemple, certains utilisateurs peuvent utiliser l'authentification par clé publique à l'aide de la base de données locale et d'autres utilisateurs peuvent utiliser des mots de passe avec RADIUS. Nous n'avons pas modifié de commandes.
Exigences relatives à l'utilisateur local et au mot de passe d'activation	9.17(1)	Pour les utilisateurs locaux et le mot de passe d'activation, les exigences de mot de passe suivantes ont été ajoutées : • Longueur du mot de passe : au moins 8 caractères. Auparavant, le minimum était de 3 caractères. • Caractères répétitifs et séquentiels : trois caractères ASCII ou plus consécutifs ne sont pas autorisés. Par exemple, les mots de passe suivants seront refusés : • **abc**utilisateur1 • utilisateur**543** • utilisateur**aaaa** • utilisateur2**666** Commandes nouvelles/modifiées : **enable password**, **username**

Nom de la caractéristique	Versions de plateforme	Description
Modifications du verrouillage de l'utilisateur local	9.17(1)	L'ASA peut verrouiller les utilisateurs locaux après un nombre configurable de tentatives de connexion échouées. Cette fonctionnalité ne s'applique pas aux utilisateurs ayant le niveau de privilège 15. De plus, un utilisateur serait verrouillé indéfiniment jusqu'à ce qu'un administrateur déverrouille son compte. Désormais, les utilisateurs seront déverrouillés après 10 minutes, à moins qu'un administrateur n'utilise la commande **clear aaa local user lockout** avant. Les utilisateurs ayant le niveau de privilège 15 sont également concernés par le paramètre de verrouillage. Commandes nouvelles ou modifiées : **aaa local authentication attempts max-fail** , **show aaa local user**
Invite de modification du mot de passe SSH et Telnet	9.17(1)	La première fois qu'un utilisateur local se connecte à l'ASA à l'aide de SSH ou de Telnet, il est invité à changer de mot de passe. Il sera également invité à se connecter pour la première fois après qu'un administrateur aura modifié son mot de passe. Si l'ASA se recharge, les utilisateurs ne seront pas invités, même s'il s'agit de leur première connexion. Commandes nouvelles ou modifiées : **show aaa local user**



CHAPITRE 38

Serveurs RADIUS pour AAA

Ce chapitre décrit comment configurer les serveurs RADIUS pour AAA.

- À propos des serveurs RADIUS pour AAA, à la page 1215
- Lignes directrices relatives aux serveurs RADIUS pour AAA, à la page 1228
- Configurer les serveurs RADIUS pour AAA, à la page 1228
- Supervision des serveurs RADIUS pour AAA, à la page 1235
- Historique des serveurs RADIUS pour AAA, à la page 1236

À propos des serveurs RADIUS pour AAA

L'ASA prend en charge les serveurs RADIUS conformes à la norme RFC suivants pour AAA :

- Cisco Secure ACS 3.2, 4.0, 4.1, 4.2 et 5.x
- Cisco Identity Services Engine (ISE)
- RSA RADIUS dans RSA Authentication Manager 5.2, 6.1 et 7.x
- Microsoft

Méthodes d'authentification prises en charge

L'ASA prend en charge les méthodes d'authentification suivantes avec les serveurs RADIUS :

- PAP : pour tous les types de connexion.
- CHAP et MS-CHAPv1 : pour les connexions L2TP-over-IPsec.
- MS-CHAPv2 : pour les connexions L2TP sur IPsec et pour les connexions d'accès à distance IPsec normales lorsque la fonctionnalité de gestion des mots de passe est activée. Vous pouvez également utiliser MS-CHAPv2 avec des connexions sans client.
- Modes de mandataire pour l'authentification : pour les connexions RADIUS à Active-Directory, RADIUS à RSA/SDI, RADIUS à serveur de jeton et RSA/SDI à RADIUS.

Remarque Pour activer MS-CHAPv2 comme protocole utilisé entre l'ASA et le serveur RADIUS pour une connexion VPN, la gestion des mots de passe doit être activée dans les attributs généraux du groupe de tunnels. L'activation de la gestion des mots de passe génère une demande d'authentification MS-CHAPv2 de l'ASA au serveur RADIUS. Consultez la description de la commande **password-management** pour en savoir plus.

Si vous utilisez la double authentification et activez la gestion des mots de passe dans le groupe de tunnels, les demandes d'authentification principale et secondaire incluent les attributs de demande MS-CHAPv2. Si un serveur RADIUS ne prend pas en charge MS-CHAPv2, vous pouvez configurer ce serveur pour envoyer une demande d'authentification non MS-CHAPv2 à l'aide de la commande **no mschapv2-capable**.

Autorisation des utilisateurs pour les connexions VPN

L'ASA peut utiliser des serveurs RADIUS pour l'autorisation des utilisateurs d'accès à distance VPN et des sessions de mandataire direct de pare-feu à l'aide d'ACL dynamiques ou de noms d'ACL par utilisateur. Pour mettre en œuvre des ACL dynamiques, vous devez configurer le serveur RADIUS pour les prendre en charge. Lorsque l'utilisateur s'authentifie, le serveur RADIUS envoie une ACL téléchargeable ou un nom d'ACL à l'ASA. L'accès à un service donné est autorisé ou refusé par l'ACL. L'ASA supprime l'ACL lorsque la session d'authentification expire.

En plus des ACL, l'ASA prend en charge de nombreux autres attributs pour l'autorisation et la définition des autorisations pour l'accès à distance au VPN et les sessions de mandataire direct par le pare-feu.

Ensembles d'attributs RADIUS pris en charge

L'ASA prend en charge les ensembles d'attributs RADIUS suivants :

- Attributs d'authentification définis dans les RFC 2138 et 2865.
- Attributs de traçabilité définis dans les RFC 2139 et 2866.
- Attributs RADIUS pour la prise en charge du protocole tunnelé, définis dans les RFC 2868 et 6929.
- Attributs spécifiques au fournisseur (VSA) Cisco IOS, identifiés par l'ID de fournisseur RADIUS 9.
- VSA liés au VPN Cisco, identifiés par l'ID de fournisseur RADIUS 3076.
- VSA Microsoft, définis dans la RFC 2548.

Attributs d'autorisation RADIUS pris en charge

L'autorisation désigne le processus d'application d'autorisations ou d'attributs. Un serveur RADIUS défini comme serveur d'authentification applique des autorisations ou des attributs s'ils sont configurés. Ces attributs ont l'ID de prestataire 3076.

Le tableau suivant répertorie les attributs RADIUS pris en charge qui peuvent être utilisés pour l'autorisation de l'utilisateur.



Remarque Les noms d'attributs RADIUS ne contiennent pas le préfixe cVPN3000. Cisco Secure ACS 4.x prend en charge cette nouvelle nomenclature, mais les noms d'attributs dans les versions ACS antérieures à la version 4.0 incluent toujours le préfixe cVPN3000. Les ASA appliquent les attributs RADIUS en fonction de l'ID numérique de l'attribut, et non du nom de l'attribut.

Tous les attributs répertoriés dans le tableau suivant sont des attributs en aval envoyés du serveur RADIUS à l'ASA, à l'exception des numéros d'attribut suivants : 146, 150, 151 et 152. Ces numéros d'attribut sont des attributs en amont qui sont envoyés de l'ASA au serveur RADIUS. Les attributs RADIUS 146 et 150 sont envoyés de l'ASA au serveur RADIUS pour les demandes d'authentification et d'autorisation. Les quatre attributs précédemment répertoriés sont envoyés de l'ASA au serveur RADIUS pour les demandes de démarrage, de mise à jour provisoire et d'arrêt de gestion. Les attributs RADIUS en amont 146, 150, 151 et 152 ont été introduits dans la version 8.4(3).

Tableau 47 : Attributs d'autorisation RADIUS pris en charge

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Heures d'accès	O	1	Chaîne	Unique	Nom de la plage temporelle, par exemple, Heures ouvrables
Liste d'accès entrant	O	86	Chaîne	Unique	ID d'ACL
Liste d'accès sortante	O	87	Chaîne	Unique	ID d'ACL
Ensembles des adresses	O	217	Chaîne	Unique	Nom de l'ensemble d'adresses IP locales
Allow-Network-Extension-Mode	O	64	Booléen	Unique	0 = Désactivé 1 = Activé
Authenticated-User-Idle-Timeout	O	50	nombre entier	Unique	1 à 35791394 minutes
Authorization-DN-Field	O	67	Chaîne	Unique	Valeurs possibles : UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, use-entire-name
Authorization-Required		66	nombre entier	Unique	0 = non 1 = oui
Authorization-Type	O	65	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP
Banner1	O	15	Chaîne	Unique	Chaîne de caractères de bannière à afficher pour les sessions d'accès à distance VPN Cisco : IPsec IKEv1, Secure Client (services client sécurisés) SSL-TLS/DTLS/IKEv2 et Clientless SSL

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Banner2	O	36	Chaîne	Unique	Chaîne de caractères de bannière à afficher pour les sessions d'accès à distance VPN Cisco : IPsec IKEv1, Secure Client (services client sécurisés) SSL-TLS/DTLS/IKEv2 et Clientless SSL La chaîne Bannière2 est concaténée à la chaîne Bannière1, si elle est configurée.
Cisco-IP-Phone-Bypass	O	51	nombre entier	Unique	0 = Désactivé 1 = Activé
Cisco-LEAP-Bypass	O	75	nombre entier	Unique	0 = Désactivé 1 = Activé
Type de client	O	150	nombre entier	Unique	1 = Cisco VPN Client (IKEv1) 2 = Secure Client (services client sécurisés) SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = Secure Client (services client sécurisés) IPsec VPN (IKEv2)
Client-Type-Version-Limiting	O	77	Chaîne	Unique	Chaîne du numéro de version de VPN IPSec
DHCP-Network-Scope	O	61	Chaîne	Unique	Adresse IP
Extended-Authentication-On-Rekey	O	122	nombre entier	Unique	0 = Désactivé 1 = Activé
Framed-Interface-Id	O	96	Chaîne	Unique	ID de l'interface IPv6 affectée. Se combine avec Framed-IPv6-Prefix pour créer une adresse IPv6 complète. Par exemple : Framed-Interface-ID=1:1:1:1 combiné avec Framed-IPv6-Prefix= 2001:0db8::/64 donne l'adresse IP attribuée 2001:0db8::1:1:1:1.
Framed-IPv6-Prefix	O	97	Chaîne	Unique	Préfixe et longueur IPv6 affectées. À combiner avec Framed-Interface-Id pour créer une adresse IPv6 complète. Par exemple : prefix 2001:0db8::/64 combiné avec Framed-Interface-Id=1:1:1:1:1 donne l'adresse IP 2001:0db8::1:1:1:1. Vous pouvez utiliser cet attribut pour attribuer une adresse IP sans utiliser Framed-Interface-Id, en attribuant l'adresse IPv6 complète avec la longueur de préfixe /128, par exemple, Framed-IPv6-Prefix=2001:0db8::1/128.

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Politique de groupe	O	25	Chaîne	Unique	Définit la politique de groupe pour la session VPN d'accès à distance. Pour les versions 8.2.x et ultérieures, utilisez cet attribut au lieu de IETF-Radius-Class. Vous pouvez utiliser l'un des formats suivants : • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*;
IE-Proxy-Bypass-Local		83	nombre entier	Unique	0 = aucun 1 = local
IE-Proxy-Exception-List		82	Chaîne	Unique	Nouvelle liste de domaines DNS séparés par des lignes (\n)
URL-PAC-IE-Proxy	O	133	Chaîne	Unique	Chaîne d'adresse PAC
IE-Proxy-Server		80	Chaîne	Unique	Adresse IP
IE-Proxy-Server-Policy		81	nombre entier	Unique	1 = Aucune modification 2 = Aucun mandataire 3 = Détection automatique 4 = Utiliser le paramètre du concentrateur
IKE-KeepAlive-Confidence-Interval	O	68	nombre entier	Unique	10 à 300 secondes
IKE-Keepalive-Retry-Interval	O	84	nombre entier	Unique	2 à 10 secondes
IKE-Keep-Alives	O	41	Booléen	Unique	0 = Désactivé 1 = Activé
Intercept-DHCP-Configure-Msg	O	62	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Allow-Passwd-Store	O	16	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Authentication		13	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP (autorisation seulement) 3 = Domaine NT 4 = SDI 5 = Interne 6 = RADIUS avec expiration 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	O	42	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Backup-Server-List	O	60	Chaîne	Unique	Adresses du serveur (délimitées par un espace)
IPsec-Backup-Servers	O	59	Chaîne	Unique	1 = Utiliser la liste configurée par le client 2 = Désactiver et effacer la liste du client 3 = Utiliser la liste du serveur de sauvegarde

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IPsec-Client-Firewall-Filter-Name		57	Chaîne	Unique	Spécifie le nom du filtre à envoyer au client en tant que politique de pare-feu
IPsec-Client-Firewall-Filter-Optional	O	58	nombre entier	Unique	0 = obligatoire 1 = facultatif
IPsec-Default-Domain	O	28	Chaîne	Unique	Spécifie le nom de domaine par défaut à envoyer au client (1 à 255 caractères).
IPsec-IKE-Peer-ID-Check	O	40	nombre entier	Unique	1 = Obligatoire 2 = Si pris en charge par le certificat homologue 3 = Ne pas vérifier
IPsec-IP-Compression	O	39	nombre entier	Unique	0 = Désactivé 1 = Activé
IPsec-Mode-Config	O	31	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP	O	34	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP-Port	O	35	nombre entier	Unique	4001à 49151. La valeur par défaut est 10 000.
IPsec-Required-Client-Firewall-Capability	O	56	nombre entier	Unique	0 = Aucune 1 = Politique définie par le micro-logiciel Are You There (Ayt) distant 2 = Politique transmise au CPP 4 = Politique du serveur
IPsec-Sec-association		12	Chaîne	Unique	Nom de l'association de sécurité
IPsec-Split-DNS-Names	O	29	Chaîne	Unique	Spécifie la liste des noms de domaines secondaires à envoyer au client (1 à 255 caractères).
IPsec-Split-Tunneling-Policy	O	55	nombre entier	Unique	0 = Aucun tunnellisation fractionnée 1 = Tunnellisation fractionnée 2 = LAN local autorisé
IPsec-Split-Tunnel-List	O	27	Chaîne	Unique	Spécifie le nom du réseau ou de la liste de contrôle d'accès qui décrit la liste d'inclusion du tunnel fractionné.
IPsec-Tunnel-Type	O	30	nombre entier	Unique	1 = LAN à LAN 2 = Accès à distance
IPsec-User-Group-Lock		33	Booléen	Unique	0 = Désactivé 1 = Activé
IPv6-Address-Pools	O	218	Chaîne	Unique	Name of IP local pool-IPv6
IPv6-VPN-Filter	O	219	Chaîne	Unique	Valeur ACL
L2TP-Encryption		21	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 128 bits 8 = Stateless-Req 15 = 40/128-Encr/Stateless-Req

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
L2TP-MPPC-Compression		38	nombre entier	Unique	0 = Désactivé 1 = Activé
Member-Of	O	145	Chaîne	Unique	Chaîne délimitée par des virgules, par exemple : `Engineering, Sales` Attribut administratif qui peut être utilisé dans les politiques d'accès dynamique. Elle ne définit pas de politique de groupe.
MS-Client-Subnet-Mask	O	63	Booléen	Unique	Une adresse IP
NAC-Default-ACL		92	Chaîne		ACL
NAC-Enable		89	nombre entier	Unique	0 = non 1 = oui
NAC-Revalidation-Timer		91	nombre entier	Unique	300 à 86 400 secondes
NAC-Settings	O	141	Chaîne	Unique	Nom de la politique NAC
NAC-Status-Query-Timer		90	nombre entier	Unique	30 à 1800 secondes
Perfect-Forward-Secrecy-Enable	O	88	Booléen	Unique	0 = non 1 = oui
PPTP-Encryption		20	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 128 bits 8 = Stateless-Requis 15= 40/128-Encr/Stateless-Req
PPTP-MPPC-Compression		37	nombre entier	Unique	0 = Désactivé 1 = Activé
Primary-DNS	O	5	Chaîne	Unique	Une adresse IP
Primary-WINS	O	7	Chaîne	Unique	Une adresse IP
Privilege-Level	O	220	nombre entier	Unique	Un nombre entier entre 0 et 15.
Required-Client-Firewall-Vendor-Code	O	45	nombre entier	Unique	1 = Cisco Systems (avec Cisco Integrated Client) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems (avecCisco Intrusion Prevention Security Agent)
Required-Client-Firewall-Description	O	47	Chaîne	Unique	Chaîne

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Required-Client-Firewall-Product Code	O	46	nombre entier	Unique	Produits Cisco Systems : 1 = Cisco Intrusion Prevention Security Agent ou Cisco Integrated Client (CIC) Produits Zone Labs : 1 = Alarme de zone 2 = Alarme de zone Pro 3 = Zone Labs Integrity Produit NetworkICE : 1 = NoirIce Defender/Agent Produits Sygate : 1 = Personal Firewall 2 = Personal Firewall Pro 3 = security Agent
Required-Individual-User-Auth	O	49	nombre entier	Unique	0 = Désactivé 1 = Activé
Require-HW-Client-Auth	O	48	Booléen	Unique	0 = Désactivé 1 = Activé
Secondary-DNS	O	6	Chaîne	Unique	Une adresse IP
Secondary-WINS	O	8	Chaîne	Unique	Une adresse IP
SEP-Card-Attribution		9	nombre entier	Unique	Non utilisé
Sous-type de session	O	152	nombre entier	Unique	0 = Aucun 1 = Sans client 2 = Client 3 = Client seulement Le sous-type de session s'applique uniquement lorsque l'attribut de type de session (151) a les valeurs suivantes : 1, 2, 3 et 4.
Type de séance	O	151	nombre entier	Unique	0 = Aucun 1 = Secure Client (services client sécurisés) VPN SSL 2 = Secure Client (services client sécurisés) VPN IPSec (IKEv2) 3 = VPN SSL sans client 4 = serveur mandataire de messagerie sans client 5 = Client Cisco VPN (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = Équilibrage de charge VPN
Connexions simultanées	O	2	nombre entier	Unique	0 à 2147483647
Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent
Smart-Tunnel-Auto	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage automatique
Smart-Tunnel-Auto-Signon-Enable	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique de tunnel Smart à côté du nom de domaine

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Strip-Realm	O	135	Booléen	Unique	0 = Désactivé 1 = Activé
SVC-Ask	O	131	Chaîne	Unique	0 = Désactivé 1 = Activé 3 = Active le service par défaut 5 = Active l'absence de client par défaut (2 et 4 non utilisés)
SVC-Ask-Timeout	O	132	nombre entier	Unique	5 à 120 secondes
Client-SVC-DPD-Interval	O	108	nombre entier	Unique	0 = Désactivé, 5 à 3 600 secondes
Passerelle-SVC-DPD-Interval	O	109	nombre entier	Unique	0 = Désactivé) 5 à 3 600 secondes
SVC-DTLS	O	123	nombre entier	Unique	0 = faux 1 = vrai
SVC-Keepalive	O	107	nombre entier	Unique	0 = Désactivé, 15–600 secondes
SVC-Modules	O	127	Chaîne	Unique	Chaîne de caractères (nom d'un module)
SVC-MTU	O	125	nombre entier	Unique	Valeur MTU 256 à 1406 en octets
SVC-Profiles	O	128	Chaîne	Unique	Chaîne de caractères (nom d'un profil)
SVC-Rekey-Time	O	110	nombre entier	Unique	0 = Désactivé 1 à 10 080 minutes
Tunnel Group Name	O	146	Chaîne	Unique	1 à 253 caractères
Tunnel-Group-Lock	O	85	Chaîne	Unique	Nom du groupe de tunnels ou « none » (aucun)
Tunneling-Protocoles	O	11	nombre entier	Unique	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 et 4 s'excluent mutuellement. 0 à 11, 16 à 27, 32 à 43 et 48 à 59 sont des valeurs autorisées.
Use-Client-Address		17	Booléen	Unique	0 = Désactivé 1 = Activé
VLAN	O	140	nombre entier	Unique	0 à 4094
WebVPN-Access-List	O	73	Chaîne	Unique	Nom de la liste d'accès
WebVPN ACL	O	73	Chaîne	Unique	Nom d'une ACL WebVPN sur le périphérique
WebVPN-ActiveX-Relay	O	137	nombre entier	Unique	0 = Désactivé Sinon = Activé
WebVPN-Apply-ACL	O	102	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Auto-HTTP-Signon	O	124	Chaîne	Unique	Réservé
WebVPN-Citrix-Metaframe-Enable	O	101	nombre entier	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-Content-Filter-Parameters	O	69	nombre entier	Unique	1 = Java ActiveX 2 = Java Script 4 = Image 8 = Témoins dans les images
WebVPN-Customization	O	113	Chaîne	Unique	Nom de la personnalisation
WebVPN-Default-Homepage	O	76	Chaîne	Unique	Une URL telle que http://exemple-exemple.com
WebVPN-Deny-Message	O	116	Chaîne	Unique	Chaîne de caractères valide (jusqu'à 500 caractères)
WebVPN-Download_Max-Size	O	157	nombre entier	Unique	0x7fffffff
WebVPN-File-Access-Enable	O	94	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Browsing-Enable	O	96	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Entry-Enable	O	95	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	O	78	Chaîne	Unique	DNS/IP séparés par des virgules avec un caractère générique facultatif (*) (par exemple *.cisco.com, 192.168.1.*, wwwin.cisco.com)
WebVPN-Hidden-Shares	O	126	nombre entier	Unique	0 = aucun 1 = visible
WebVPN-Home-Page-Use-Smart-Tunnel	O	228	Booléen	Unique	Activé si la page d'accueil sans client doit être affichée par l'intermédiaire de Smart Tunnel.
WebVPN-HTML-Filter	O	69	Bitmap	Unique	1 = ActiveX Java 2 = Scripts 4 = Image 8 = Témoins
WebVPN-HTTP-Compression	O	120	nombre entier	Unique	0 = Désactivé 1 = Décompression
WebVPN-HTTP-Proxy-IP-Address	O	74	Chaîne	Unique	DNS/IP séparé par des virgules:port, avec le préfixe http= ou https= (par exemple http=10.10.10:80, https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert-Interval	O	148	nombre entier	Unique	0 à 30. 0 = Désactivé.
WebVPN-Keepalive-Ignore	O	121	nombre entier	Unique	0 à 900
WebVPN-Macro-Substitution	O	223	Chaîne	Unique	Illimité.
WebVPN-Macro-Substitution	O	224	Chaîne	Unique	Illimité.
WebVPN-Port-Forwarding-Enable	O	97	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	O	98	nombre entier	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-Port-Forwarding-HTTP-Proxy	O	99	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-List	O	72	Chaîne	Unique	Nom de la liste de transferts de port
WebVPN-Port-Forwarding-Name	O	79	Chaîne	Unique	Nom de chaîne de caractères (par exemple, « Corporate-Apps »). Ce texte remplace la chaîne par défaut « Application Access » dans la page d'accueil du portail sans client.
WebVPN-post-maximum-taille	O	159	nombre entier	Unique	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	O	149	nombre entier	Unique	0 à 30. 0 = Désactivé.
WebVPN Smart-Card-Removal-Disconnect	O	225	Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent
WebVPN-Smart-Tunnel-Auto-Sign-On	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique de Smart Tunnel ajouté par le nom de domaine
WebVPN-Smart-Tunnel-Auto-Start	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage automatique
WebVPN-Smart-Tunnel-Tunnel-Policy	O	227	Chaîne	Unique	Un des choix « e networkname », « i networkname » ou « a », où networkname est le nom d'une liste de réseaux Smart Tunnels, e indiquant le tunnel exclu, i le tunnel spécifié et a indique tous les tunnels.
WebVPN-SSL-VPN-Client-Enable	O	103	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Keep-Installation	O	105	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Required	O	104	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSO-Server-Name	O	114	Chaîne	Unique	Chaîne de caractères valide
WebVPN-Storage-Key	O	162	Chaîne	Unique	
WebVPN-Storage-Objects	O	161	Chaîne	Unique	
WebVPN-SVC-Keepalive-Frequency	O	107	nombre entier	Unique	15 à 600 secondes, 0 = désactivé
WebVPN-SVC-Client-DPD-Frequency	O	108	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé
WebVPN-SVC-DTLS-Enable	O	123	nombre entier	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-SVC-DTLS-MTU	O	125	nombre entier	Unique	La valeur MTU est comprise entre 256 et 1406 octets.
WebVPN-SVC-Gateway-DPD-Frequency	O	109	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé
WebVPN-SVC-Rekey-Time	O	110	nombre entier	Unique	4 à 10 080 minutes, 0 = Désactivé
WebVPN-SVC-Rekey-Method	O	111	nombre entier	Unique	0 (désactivé), 1 (SSL), 2 (nouveau tunnel)
WebVPN-SVC-Compression	O	112	nombre entier	Unique	0 (Désactivé), 1 (Décompression)
WebVPN-UNIX-Group-ID (GID)	O	222	nombre entier	Unique	ID de groupe UNIX valides
WebVPN-UNIX-User-ID (UIDs)	O	221	nombre entier	Unique	ID d'utilisateur UNIX valides
WebVPN-Upload-Max-Size	O	158	nombre entier	Unique	0x7fffffff
WebVPN-URL-Entry-Enable	O	93	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-URL-List	O	71	Chaîne	Unique	Nom de la liste d'URL
WebVPN-User-Storage	O	160	Chaîne	Unique	
WebVPN-VDI	O	163	Chaîne	Unique	Liste des paramètres

Attributs d'autorisation RADIUS IETF pris en charge

Le tableau suivant présente les attributs RADIUS IETF pris en charge.

Tableau 48 : Attributs RADIUS IETF pris en charge

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IETF-Radius-Class	O	25		Unique	Pour les versions 8.2.x et ultérieures, nous vous recommandons d'utiliser l'attribut Group-Policy (VSA 3076, n° 25) : • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*
IETF-Radius-Filter-Id	O	11	Chaîne	Unique	Nom de l'ACL défini sur l'ASA, qui s'applique uniquement aux clients SSL VPN et IPsec du tunnel complet.
IETF-Radius-Framed-IP-Address	O	S.O.	Chaîne	Unique	Une adresse IP

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IETF-Radius-Framed-IP-Netmask	O	S.O.	Chaîne	Unique	Un masque d'adresse IP
IETF-Radius-Idle-Timeout	O	28	nombre entier	Unique	Secondes
IETF-Radius-Service-Type	O	6	nombre entier	Unique	Secondes. Valeurs possibles pour le type de service : • .Administrative : l'utilisateur a accès à l'invite de configuration. • .NAS-Prompt : l'utilisateur a accès à l'invite d'exécution. • .remote-access : l'utilisateur a accès au réseau.
IETF-Radius-Session-Timeout	O	27	nombre entier	Unique	Secondes

Codes de motif de déconnexion comptable RADIUS

Ces codes sont renvoyés si l'ASA rencontre une déconnexion lors de l'envoi de paquets :

Code de motif de déconnexion
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14

Code de motif de déconnexion
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

Lignes directrices relatives aux serveurs RADIUS pour AAA

Cette section décrit les lignes directrices et les limites que vous devez vérifier avant de configurer les serveurs RADIUS pour l'AAA.

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 4 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple.
- La longueur maximale de la charge utile RADIUS est de 4096 octets.

Configurer les serveurs RADIUS pour AAA

Cette section décrit comment configurer les serveurs RADIUS pour AAA.

Procédure

Étape 1 Chargez les attributs ASA dans le serveur RADIUS. La méthode que vous utilisez pour charger les attributs dépend du type de serveur RADIUS que vous utilisez :

- Si vous utilisez Cisco ACS : le serveur intègre déjà ces attributs. Vous pouvez ignorer cette étape.
- Pour les serveurs RADIUS d'autres fournisseurs (par exemple, le service d'authentification Internet Microsoft) : vous devez définir manuellement chaque attribut ASA. Pour définir un attribut, utilisez le nom ou le numéro d'attribut, le type, la valeur et le code du fournisseur (3076).

Étape 2 Configurer les groupes de serveurs RADIUS, à la page 1229.

Étape 3 Ajouter un serveur RADIUS à un groupe, à la page 1232.

Configurer les groupes de serveurs RADIUS

Si vous souhaitez utiliser un serveur RADIUS externe pour l'authentification, l'autorisation ou la gestion de comptes, vous devez d'abord créer au moins un groupe de serveurs RADIUS par protocole AAA et ajouter un ou plusieurs serveurs à chaque groupe.

Procédure

Étape 1 Créez le groupe de serveurs AAA RADIUS.

aaa-server *group_name* **protocol radius**

Exemple :

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)#
```

Lorsque vous saisissez la commande **aaa-server protocol**, vous passez en mode de configuration du groupe aaa-server.

Étape 2 (Facultatif) Précisez le nombre maximum de transactions AAA échouées avec un serveur RADIUS du groupe avant d'essayer le serveur suivant.

max-failed-attempts *number*

La plage se situe entre 1 et 5. La valeur par défaut est de 3.

Si vous avez configuré une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement), et que tous les serveurs du groupe ne répondent pas ou que leurs réponses ne sont pas valides, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la commande **reactivation-mode** à l'étape suivante.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

Exemple :

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

Étape 3 (Facultatif) Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

Lieu :

- **depletion** [**deadtime** *minutes*] réactive les serveurs défaillants seulement après que tous les serveurs du groupe sont inactifs. Il s'agit du mode de réactivation par défaut. Vous pouvez préciser la durée, entre 0 et 1 440 minutes, qui s'écoule entre la désactivation du dernier serveur du groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort. La valeur par défaut est 10 minutes.

- **timed** réactive les serveurs défaillants après 30 secondes de temps d'arrêt.

Exemple :

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

Étape 4 (Facultatif) Envoyez des messages de traçabilité à tous les serveurs du groupe.

accounting-mode simultaneous

Pour rétablir la valeur par défaut d'envoi de messages uniquement au serveur actif, saisissez la commande **accounting-mode single**.

Exemple :

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

Étape 5 (Facultatif) Activez la génération périodique de messages RADIUS interim-accounting-update.

interim-accounting-update [**periodic** [*hours*]]

ISE gère un répertoire des sessions actives en fonction des enregistrements de traçabilité qu'il reçoit des périphériques NAS comme l'ASA. Cependant, si ISE ne reçoit aucune indication que la session est toujours active (message de traçabilité ou transactions de posture) pendant une période de 5 jours, il supprimera l'enregistrement de session de sa base de données. Pour vous assurer que les connexions VPN de longue durée ne sont pas supprimées, configurez le groupe pour envoyer des messages interim-accounting-update périodiques à ISE pour toutes les sessions actives.

- **periodic** [*hours*] permet la génération et la transmission périodiques des enregistrements de comptabilité pour chaque session VPN configurée pour envoyer des enregistrements de comptabilité au groupe de serveurs en question. Vous pouvez éventuellement inclure l'intervalle, en heures, pour l'envoi de ces mises à jour. La valeur par défaut est de 24 heures, la plage est comprise entre 1 et 120.
- (Aucun paramètre.) Si vous utilisez cette commande sans le mot clé **periodic**, l'ASA envoie des messages interim-accounting-update uniquement lorsqu'une connexion de tunnel VPN est ajoutée à une session VPN sans client. Lorsque cela se produit, la mise à jour de comptabilité est générée afin d'informer le serveur RADIUS de la nouvelle adresse IP attribuée.

Exemple :

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

Étape 6 (Facultatif) Activez les services d'autorisation dynamique RADIUS (changement d'autorisation, CoA, d'ISE) pour le groupe de serveurs AAA.

dynamic-authorization [**port** *number*]

La définition d'un port est facultative. La valeur par défaut est 1700, la plage est comprise entre 1024 et 65535.

Lorsque vous utilisez le groupe de serveurs dans un tunnel VPN, le groupe de serveurs RADIUS sera enregistré pour la notification CoA et l'ASA écoutera le port pour détecter les mises à jour de politique CoA d'ISE. Activez l'autorisation dynamique uniquement si vous utilisez ce groupe de serveurs dans un VPN d'accès à distance en conjonction avec l'ISE.

Exemple :

```
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

Étape 7 (Facultatif) Si vous ne souhaitez pas utiliser ISE pour l'authentification, activez le mode d'autorisation seulement pour le groupe de serveurs RADIUS. (Activez le mode d'autorisation uniquement si vous utilisez ce groupe de serveurs dans un VPN d'accès à distance en conjonction avec l'ISE.)

authorize-only

Cela indique que lorsque ce groupe de serveurs est utilisé pour l'autorisation, le message de demande d'accès RADIUS sera généré en tant que demande « Autorize Only » (Autorisation uniquement), par opposition aux méthodes de mot de passe configurées pour le serveur AAA. Si vous configurez un mot de passe commun à l'aide de la commande **radius-common-pw** pour le serveur RADIUS, il sera ignoré.

Par exemple, vous utiliserez le mode d'autorisation seulement si vous souhaitez utiliser des certificats pour l'authentification plutôt que ce groupe de serveurs. Vous utiliserez toujours ce groupe de serveurs pour l'autorisation et la gestion de comptes dans le tunnel VPN.

Exemple :

```
ciscoasa(config-aaa-server-group)# authorize-only
```

Étape 8 (Facultatif) Fusionnez une ACL téléchargeable avec l'ACL reçue dans la paire AV de Cisco à partir d'un paquet RADIUS.

merge-dacl {**before-avpair** | **after-avpair**}

Exemple :

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

Cette option s'applique uniquement aux connexions VPN. Pour les utilisateurs de VPN, les ACL peuvent prendre la forme d'ACL de paire attribut/valeur de Cisco, d'ACL téléchargeables et d'une ACL configurée sur l'ASA. Cette option détermine si l'ACL téléchargeable et l'ACL de la paire attribut/valeur sont fusionnées, et ne s'applique à aucune ACL configurée sur l'ASA.

Le paramètre par défaut est **no merge dacl**, ce qui indique que les ACL téléchargeables ne seront pas fusionnées avec les ACL de paire attribut/valeur de Cisco. Si une paire AV et une ACL téléchargeable sont reçues, la paire AV a la priorité et est utilisée.

L'option **before-avpair** signifie que les entrées d'ACL téléchargeables doivent être placées avant les entrées de la paire d'AV de Cisco.

L'option **after-avpair** signifie que les entrées d'ACL téléchargeables doivent être placées après les entrées de la paire d'AV de Cisco.

Exemples

L'exemple suivant montre comment ajouter un groupe RADIUS avec un seul serveur :

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
```

```
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

L'exemple suivant montre comment configurer un groupe de serveurs ISE pour les mises à jour d'autorisation dynamique (CoA) et la comptabilité périodique horaire. La configuration du groupe de tunnels qui configure l'authentification par mot de passe avec ISE est incluse.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

L'exemple suivant montre comment configurer un groupe de tunnels pour la validation et l'autorisation des certificats locaux avec ISE. Incluez la commande authorize-only dans la configuration du groupe de serveurs, car le groupe de serveurs ne sera pas utilisé pour l'authentification.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Ajouter un serveur RADIUS à un groupe

Pour ajouter un serveur RADIUS à un groupe, procédez comme suit :

Procédure

Étape 1 Identifiez le serveur RADIUS et le groupe de serveurs AAA auquel il appartient.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

Exemple :

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

Si vous ne spécifiez pas de **(***nom d'interface***)**, l'ASA utilise la de l'interface **interne** par défaut.

Étape 2 Spécifiez comment l'ASA traite les masques réseau reçus dans une ACL téléchargeable d'un serveur RADIUS.

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

Exemple :

```
ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

Le mot clé **auto-detect** spécifie que l'ASA doit tenter de déterminer le type d'expression de masque réseau utilisé. Si l'ASA détecte une expression de masque réseau à caractère générique, il la convertit en une expression de masque réseau standard.

Le mot clé **standard** spécifie que l'ASA suppose que les ACL téléchargeables reçues du serveur RADIUS contiennent uniquement des expressions de masque réseau standard. Aucune conversion des expressions de masque réseau à caractère générique n'est effectuée.

Le mot clé **wildcard** spécifie que l'ASA suppose que les ACL téléchargeables reçues du serveur RADIUS contiennent uniquement des expressions de masque réseau à caractère générique et les convertit toutes en des expressions de masque réseau standard lorsque les ACL sont téléchargées.

Étape 3 Spécifiez un mot de passe commun à utiliser pour tous les utilisateurs qui accèdent à un serveur d'autorisation RADIUS par l'intermédiaire de l'ASA.

radius-common-pw *string*

Exemple :

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

L'argument *string* est un mot clé alphanumérique sensible à la casse d'un maximum de 127 caractères à utiliser comme mot de passe commun pour toutes les transactions d'autorisation avec le serveur RADIUS.

Étape 4 Activez les demandes d'authentification MS-CHAPv2 sur le serveur RADIUS.

mschapv2-capable

Exemple :

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

Étape 5 Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

timeout *seconds*

Spécifiez l'intervalle du délai d'expiration (1 à 300 secondes) du serveur; la valeur par défaut est de 10 secondes. Pour chaque transaction AAA, l'ASA relance les tentatives de connexion (en fonction de l'intervalle défini dans la commande **retry-interval**) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite spécifiée dans la commande max-failed-attempts dans le groupe de serveurs AAA, le serveur AAA est désactivé et l'ASA commence à envoyer des demandes à un autre serveur AAA s'il est configuré.

Exemple :

```
ciscoasa(config-aaa-server-host)# timeout 15
```

Étape 6 Configurez le délai entre les tentatives de reconnexion pour un serveur AAA spécifique désigné dans une commande précédente.

retry-interval *seconds*

Exemple :

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

L'argument *seconds* spécifie l'intervalle de reconnexion (1 à 10 secondes) pour la requête. Il s'agit du temps que l'ASA attend avant de réessayer une demande de connexion.

Remarque
Pour le protocole RADIUS, si le serveur répond par un message de port ICMP inaccessible, le paramètre retry-interval est ignoré et le serveur AAA passe immédiatement à l'état d'échec. S'il s'agit du seul serveur du groupe AAA, il est réactivé et une autre requête lui est envoyée. Il s'agi du comportement prévu.

Étape 7 Envoyez des messages de traçabilité à tous les serveurs du groupe.

accounting-mode simultaneous

Exemple :

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

Saisissez la commande **accounting-mode single** pour rétablir le paramètre par défaut consistant à envoyer des messages uniquement au serveur actif.

Étape 8 Spécifiez le port d'authentification comme numéro de port 1645 ou le port du serveur à utiliser pour l'authentification des utilisateurs.

authentication-port *port*

Exemple :

```
ciscoasa(config-aaa-server-host)# authentication-port 1646
```

Étape 9 Spécifiez le port de traçabilité comme numéro de port 1646 ou le port de serveur à utiliser pour la traçabilité de cet hôte.

accounting-port *port*

Exemple :

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

Étape 10 Spécifiez la valeur de clé secrète de serveur utilisée pour authentifier le serveur RADIUS auprès de l'ASA. La clé du serveur que vous configurez doit correspondre à celle configurée sur le serveur RADIUS. Si vous ne connaissez pas la valeur de la clé secrète du serveur, demandez à l'administrateur du serveur RADIUS. La longueur maximale est de 64caractères.

key

Exemple :

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

La clé du serveur que vous configurez doit correspondre à celle configurée sur le serveur RADIUS. Si vous ne connaissez pas la valeur de la clé secrète du serveur, demandez à l'administrateur du serveur RADIUS. La longueur maximale est de 64caractères.

Exemple

L'exemple suivant montre comment ajouter un serveur RADIUS à un groupe de serveurs RADIUS existant :

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# radius-common-pw myexaplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

Supervision des serveurs RADIUS pour AAA

Consultez les commandes suivantes pour superviser l'état des serveurs RADIUS pour AAA :

- **show aaa-server**

  Cette commande affiche les statistiques du serveur RADIUS configuré. Vous pouvez utiliser la commande **clear aaa-server statistics** pour réinitialiser les compteurs à zéro.

- **show running-config aaa-server**

  Cette commande montre la configuration d'exécution du serveur RADIUS.

Historique des serveurs RADIUS pour AAA

Tableau 49 : Historique des serveurs RADIUS pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs RADIUS pour AAA	7.0(1)	Décrit comment configurer les serveurs RADIUS pour AAA. Nous avons introduit les commandes suivantes : **aaa-server protocol**, **max-failed-attempts**, **reactivation-mode**, **accounting-mode simultaneous**, **aaa-server host**, **show aaa-server**, **show running-config aaa-server**, **clear aaa-server statistics**, **authentication-port**, **accounting-port**, **retry-interval**, **acl-netmask-convert**, **clear configure aaa-server**, **merge-dacl**, **radius-common-pw, key**.
Attributs propres au fournisseur de clé (VSA) envoyés dans les paquets de demande d'accès et de demande de comptabilité RADIUS à partir de l'ASA	8.4(3)	Quatre nouveaux VSA : le nom du groupe de tunnels (146) et le type de client (150) sont envoyés dans les paquets de demande d'accès RADIUS à partir de l'ASA. Le type de session (151) et le sous-type de session (152) sont envoyés dans les paquets de demande de comptabilité RADIUS à partir de l'ASA. Les quatre attributs sont envoyés pour tous les types de paquets de demande de comptabilité : Start, Interim-Update et Stop. Le serveur RADIUS (par exemple, ACS et ISE) peut alors appliquer des attributs d'autorisation et de politique ou les utiliser à des fins de comptabilité et de facturation.
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les commandes suivantes pour accepter ces nouvelles limites : **aaa-server**, **aaa-server host**.



CHAPITRE 39

Serveurs TACACS+ pour AAA

Ce chapitre décrit comment configurer les serveurs TACACS+ utilisés dans AAA.

- À propos des serveurs TACACS+ pour AAA, à la page 1237
- Lignes directrices relatives aux serveurs TACACS+ pour AAA, à la page 1239
- Configurer les serveurs TACACS+, à la page 1239
- Supervision des serveurs TACACS+ pour AAA, à la page 1242
- Historique des serveurs TACACS+ pour AAA, à la page 1243

À propos des serveurs TACACS+ pour AAA

L'ASA prend en charge l'authentification du serveur TACACS+ avec les protocoles suivants : ASCII, PAP, CHAP et MS-CHAPv1.

Attributs TACACS+

L'ASA prend en charge les attributs TACACS+. Les attributs TACACS+ séparent les fonctions d'authentification, d'autorisation et de gestion de comptes. Le protocole prend en charge deux types d'attributs : obligatoires et facultatifs. Le serveur et le client doivent comprendre un attribut obligatoire, et l'attribut obligatoire doit être appliqué à l'utilisateur. Un attribut facultatif peut ne pas être compris ou utilisé.

Remarque Pour utiliser les attributs TACACS+, assurez-vous d'avoir activé les services AAA sur le NAS.

Le tableau suivant répertorie les attributs de réponse d'autorisation TACACS+ pris en charge pour les connexions de mandataire direct.

Tableau 50 : Attributs de réponse d'autorisation TACACS+ pris en charge

Attribut	Description
acl	Identifie une ACL configurée localement à appliquer à la connexion.
idletime	Indique la durée d'inactivité en minutes qui est autorisée avant la fin de la session de l'utilisateur authentifié.

Attribut	Description
timeout	Spécifie la durée absolue en minutes pendant laquelle les informations d'authentification restent actives avant la fin de la session de l'utilisateur authentifié.

Le tableau suivant répertorie les attributs de comptabilité TACACS+ pris en charge.

.

Tableau 51 : Attributs de comptabilité TACACS+ pris en charge

Attribut	Description
bytes_in	Spécifie le nombre d'octets d'entrée transférés lors de cette connexion (enregistrements d'arrêt uniquement).
bytes_out	Spécifie le nombre d'octets de sortie transférés lors de cette connexion (enregistrements d'arrêt uniquement).
CMD	Définit la commande exécutée (comptabilisation des commandes uniquement).
disc-cause	Indique le code numérique qui identifie la raison de la déconnexion (enregistrements d'arrêt uniquement).
elapsed_time	Définit le temps écoulé en secondes pour la connexion (enregistrements d'arrêt uniquement).
foreign_ip	Indique l'adresse IP du client pour les connexions du tunnel. Définit l'adresse sur l'interface de sécurité la plus basse pour les connexions de mandataire direct.
local_ip	Spécifie l'adresse IP à laquelle le client s'est connecté pour les connexions du tunnel. Définit l'adresse sur l'interface de sécurité la plus élevée pour les connexions de mandataire direct.
Port NAS	Contient un ID de session pour la connexion.
packs_in	Indique le nombre de paquets d'entrée transférés lors de cette connexion.
packs_out	Indique le nombre de paquets de sortie transférés lors de cette connexion.
priv-level	Définit le niveau de privilège de l'utilisateur pour les demandes de comptabilité des commandes ou 1 dans le cas contraire.
rem_iddr	Indique l'adresse IP du client.
service	Spécifie le service utilisé. Toujours défini sur « shell » pour la comptabilisation des commandes uniquement.
task_id	Spécifie un ID de tâche unique pour la transaction de comptabilité.
nom d'utilisateur	Indique le nom de l'utilisateur.

Lignes directrices relatives aux serveurs TACACS+ pour AAA

Cette section décrit les lignes directrices et les limites que vous devez vérifier avant de configurer les serveurs TACACS+ pour l'AAA.

IPv6

Le serveur AAA peut utiliser une adresse IPv4 ou IPv6.

Directives supplémentaires

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 4 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple.
- Si vous configurez l'authentification à plusieurs facteurs avec ISE TACACS+ et Duo, vous devrez peut-être saisir à nouveau votre mot de passe lorsque vous établirez des connexions SSH après avoir confirmé la connexion avec Duo.
- Pour la série FPR1000, FPR2100 ou FPR3100 qui s'exécute sur l'ASA en mode appareil, vous devez vous conformer à ces conventions de nom d'utilisateur :
  - Les noms d'utilisateur doivent être valides sous Linux.
  - Ils doivent être uniquement en minuscules.
  - Ils peuvent inclure des caractères alphanumériques, des points (.) ou des tirets (-).
  - Ils ne doivent pas inclure d'autres caractères spéciaux tels que l'arobase (@) et la barre oblique (/).

Configurer les serveurs TACACS+

Cette section décrit comment configurer les serveurs TACACS+.

Procédure

Étape 1 Configurer les groupes de serveurs TACACS+, à la page 1239.

Étape 2 Ajouter un serveur TACACS+ à un groupe, à la page 1241.

Configurer les groupes de serveurs TACACS+

Si vous souhaitez utiliser un serveur TACACS+ pour l'authentification, l'autorisation ou la gestion de comptes, vous devez d'abord créer au moins un groupe de serveurs TACACS+ et ajouter un ou plusieurs serveurs à chaque groupe. Vous identifiez les groupes de serveurs TACACS+ par leur nom.

Pour ajouter un groupe de serveurs TACACS+, procédez comme suit :

Procédure

Étape 1 Identifiez le nom du groupe de serveurs et le protocole.

aaa-server *server_tag* **protocol tacacs+**

Exemple :

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

Lorsque vous saisissez la commande **aaa-server protocol**, vous passez en mode de configuration du groupe aaa-server.

Étape 2 Précisez le nombre maximum de transactions AAA échouées avec un serveur AAA du groupe avant d'essayer le serveur suivant.

max-failed-attempts *number*

Exemple :

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

L'argument *number* peut aller de 1 à 5. La valeur par défaut est de 3.

Si vous avez configuré une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement), et que tous les serveurs du groupe ne répondent pas ou que leurs réponses ne sont pas valides, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la commande **reactivation-mode** à l'étape suivante.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

Étape 3 Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

Exemple :

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

Le mot clé **depletion** réactive les serveurs défaillants uniquement après que tous les serveurs du groupe sont inactifs.

La paire mot clé-argument **deadtime** *minutes* spécifie le temps en minutes, entre 0 et 1 440, qui s'écoule entre la désactivation du dernier serveur du groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort. La valeur par défaut est 10 minutes.

Le mot clé **timed** réactive les serveurs défaillants après 30 secondes d'arrêt.

Étape 4 Envoyez des messages de traçabilité à tous les serveurs du groupe.

accounting-mode simultaneous

Exemple :

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

Pour rétablir la valeur par défaut d'envoi de messages uniquement au serveur actif, saisissez la commande **accounting-mode single**.

Exemple

L'exemple suivant montre comment ajouter un groupe TACACS+ avec un serveur principal et un serveur de sauvegarde:

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

Ajouter un serveur TACACS+ à un groupe

Pour ajouter un serveur TACACS+ à un groupe, procédez comme suit :

Procédure

Étape 1 Identifiez le serveur TACACS+ et le groupe de serveurs auquel il appartient.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

Exemple :

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

Si vous ne spécifiez pas de **(***nom d'interface***)**, l'ASA utilise la de l'interface **interne** par défaut.

Le serveur peut utiliser une adresse IPv4 ou IPv6.

Étape 2 Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

timeout *seconds*

Spécifiez l'intervalle du délai d'expiration (1 à 300 secondes) du serveur; la valeur par défaut est de 10 secondes. Pour chaque transaction AAA, l'ASA relance les tentatives de connexion (en fonction de l'intervalle défini dans la commande **retry-interval**) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite spécifiée dans la commande max-failed-attempts dans le groupe de serveurs AAA, le serveur AAA est désactivé et l'ASA commence à envoyer des demandes à un autre serveur AAA s'il est configuré.

Exemple :

```
ciscoasa(config-aaa-server-host)# timeout 15
```

Étape 3 Spécifiez le port du serveur comme numéro de port 49 ou le numéro de port TCP utilisé par l'ASA pour communiquer avec le serveur TACACS+.

server-port *port_number*

Exemple :

```
ciscoasa(config-aaa-server-host)# server-port 49
```

Étape 4 Spécifiez la valeur secrète du serveur utilisée pour authentifier le NAS auprès du serveur TACACS+.

key

Exemple :

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

Cette valeur est un mot clé alphanumérique sensible à la casse pouvant comporter jusqu'à 127 caractères, ce qui correspond à la même valeur que la clé sur le serveur TACACS+. Tout caractère au-delà de 127 est ignoré. La clé est utilisée entre le client et le serveur pour chiffrer les données entre eux et doit être identique sur les systèmes du client et du serveur. La clé ne peut pas contenir d'espaces, mais d'autres caractères spéciaux sont autorisés.

Supervision des serveurs TACACS+ pour AAA

Consultez les commandes suivantes pour superviser les serveurs TACACS+ pour AAA :

- **show aaa-server**

  Cette commande affiche les statistiques du serveur TACACS+ configuré. Saisissez la commande **clear aaa-server statistics** pour effacer les statistiques du serveur TACACS+.

- **show running-config aaa-server**

  Cette commande montre la configuration en cours d'exécution du serveur TACACS+. Saisissez la commande **clear configure aaa-server** pour effacer la configuration du serveur TACACS+.

Historique des serveurs TACACS+ pour AAA

Tableau 52 : Historique des serveurs TACACS+ pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs TACACS+	7.0(1)	Décrit comment configurer les serveurs TACACS+ pour AAA. Nous avons introduit les commandes suivantes : **aaa-server protocol**, **max-failed-attempts, reactivation-mode, accounting-mode simultaneous, aaa-server host, aaa authorization exec authentication-server**, **server-port, key**, **clear aaa-server statistics**, **clear configure aaa-server**, **show aaa-server**, **show running-config aaa-server**, **username**, **service-type**, **timeout**.
Serveurs TACACS+ avec adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les commandes suivantes pour accepter ces nouvelles limites : **aaa-server**, **aaa-server host**.



CHAPITRE 40

Serveurs LDAP pour AAA

Ce chapitre décrit comment configurer les serveurs LDAP utilisés dans AAA.

- À propos de LDAP et de l'ASA, à la page 1245
- Lignes directrices relatives aux serveurs LDAP pour AAA, à la page 1249
- Configurer les serveurs LDAP pour AAA, à la page 1249
- Supervision des serveurs LDAP pour AAA, à la page 1256
- Historique des serveurs LDAP pour AAA, à la page 1256

À propos de LDAP et de l'ASA

L'ASA est compatible avec la plupart des serveurs de répertoire LDAPv3, notamment :

- Sun Microsystems JAVA System Directory Server, fait désormais partie de l'édition Enterprise du serveur de répertoire Oracle, et anciennement nommé serveur de répertoire Sun ONE
- Microsoft Active Directory
- Novell
- OpenLDAP

Par défaut, l'ASA détecte automatiquement s'il est connecté à Microsoft Active Directory, Sun LDAP, Novell, OpenLDAP ou à un serveur de répertoire LDAPv3 générique. Toutefois, si la détection automatique ne parvient pas à déterminer le type de serveur LDAP, vous pouvez le configurer manuellement.

Fonctionnement de l'authentification avec LDAP

Pendant l'authentification, l'ASA agit comme mandataire client auprès du serveur LDAP pour l'utilisateur et s'authentifie auprès du serveur LDAP en texte brut ou à l'aide du protocole SASL. Par défaut, l'ASA transmet les paramètres d'authentification, généralement un nom d'utilisateur et un mot de passe, au serveur LDAP en texte brut.

L'ASA prend en charge les mécanismes SASL suivants, répertoriés par ordre croissant de puissance :

- Digest-MD5 : l'ASA répond au serveur LDAP par une valeur MD5 calculée à partir du nom d'utilisateur et du mot de passe.
- Kerberos : l'ASA répond au serveur LDAP en envoyant le nom d'utilisateur et le domaine à l'aide du mécanisme GSSAPI Kerberos.

L'ASA et le serveur LDAP prennent en charge toutes les combinaisons possibles de ces mécanismes SASL. Si vous configurez plusieurs mécanismes, l'ASA récupère la liste des mécanismes SASL configurés sur le serveur et définit le mécanisme d'authentification le plus puissant configuré à la fois sur l'ASA et le serveur. Par exemple, si le serveur LDAP et l'ASA prennent en charge les deux mécanismes, l'ASA sélectionne Kerberos, le plus fort des deux.

Une fois l'authentification LDAP de l'utilisateur réussie, le serveur LDAP renvoie les attributs pour l'utilisateur authentifié. Pour l'authentification VPN, ces attributs incluent généralement des données d'autorisation appliquées à la session VPN. Dans ce cas, l'utilisation de LDAP permet d'effectuer l'authentification et l'autorisation en une seule étape.

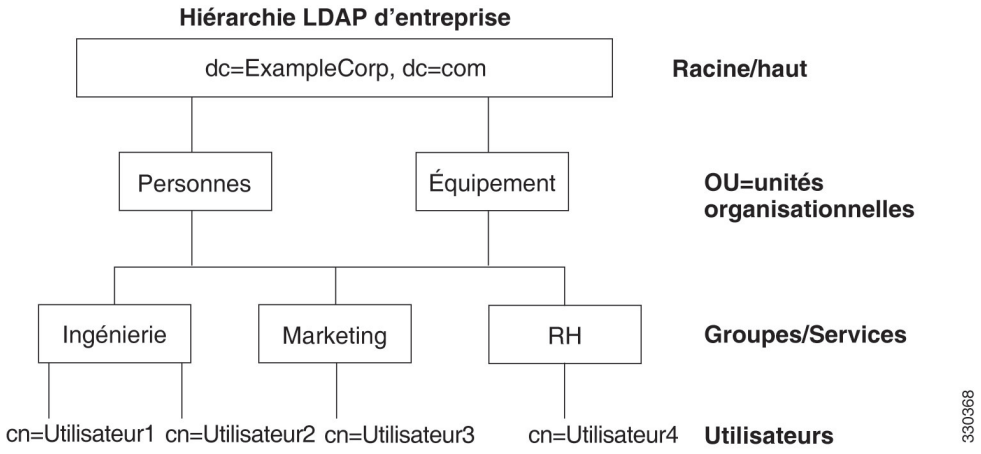
Remarque Pour en savoir plus sur LDAP, consultez les RFC 1777, 2251 et 2849.

Hiérarchie LDAP

Votre configuration LDAP doit refléter la hiérarchie logique de votre organisation. Par exemple, supposons qu'un employé de votre entreprise, Exemple Société, s'intitule Employé1. Employé 1 travaille dans le groupe d'ingénierie. Votre hiérarchie LDAP peut comporter un ou plusieurs niveaux. Vous pourriez décider de configurer une hiérarchie à un seul niveau dans laquelle Employé1 est considéré comme membre d'Exemple Société. Ou vous pouvez configurer une hiérarchie à plusieurs niveaux dans laquelle Employé1 est considéré comme un membre du service d'ingénierie, qui est lui-même membre d'une unité organisationnelle appelée Personnel, qui est elle-même membre d'Exemple Société. Consultez la figure suivante pour obtenir un exemple de hiérarchie à plusieurs niveaux.

Une hiérarchie à plusieurs niveaux est plus détaillée, mais les recherches renvoient des résultats plus rapidement dans une hiérarchie à un seul niveau.

Illustration 74 : Une hiérarchie LDAP à plusieurs niveaux



Rechercher dans la hiérarchie LDAP

L'ASA vous permet d'adapter la recherche dans la hiérarchie LDAP. Vous devez configurer les trois champs suivants sur l'ASA pour définir à quel niveau de la hiérarchie LDAP votre recherche doit commencer, son étendue et le type de renseignements que vous recherchez. Ensemble, ces champs limitent la recherche dans la hiérarchie à la partie qui inclut les autorisations des utilisateurs.

- Le DN de base LDAP définit à quel niveau de la hiérarchie LDAP le serveur doit commencer à rechercher les renseignements de l'utilisateur lorsqu'il reçoit une demande d'autorisation de l'ASA.
- La portée de recherche définit l'étendue de la recherche dans la hiérarchie LDAP. La recherche se poursuit sur ces nombreux niveaux dans la hiérarchie sous le DN de base LDAP. Vous pouvez choisir de demander au serveur de rechercher uniquement le niveau immédiatement en dessous, ou il peut rechercher dans toute la sous-arborescence. Une recherche à un seul niveau est plus rapide, mais une recherche dans la sous-arborescence est plus approfondie.
- Les attributs de nommage définissent le RDN qui identifie de manière unique une entrée dans le serveur LDAP. Les attributs de nommage courants peuvent inclure cn (nom commun), sAMAccountName et userPrincipalName.

La figure montre un exemple de hiérarchie LDAP pour l'exemple de société. Compte tenu de cette hiérarchie, vous pouvez définir votre recherche de différentes manières. Le tableau suivant présente deux exemples de configuration de recherche.

Dans le premier exemple de configuration, lorsque Employé1 établit le tunnel IPsec avec l'autorisation LDAP requise, l'ASA envoie une demande de recherche au serveur LDAP, indiquant qu'il doit rechercher Employé1 dans le groupe d'ingénierie. Cette recherche est rapide.

Dans le deuxième exemple de configuration, l'ASA envoie une demande de recherche indiquant que le serveur doit rechercher Employé1 dans l'exemple de société. Cette recherche prend plus de temps.

Tableau 53 : Exemples de configuration de recherche

Non.	DN de base LDAP	Portée de la recherche	Attribut de nommage	Résultat
1	group= Ingénierie,ou=Personnes,dc=ExempleSociété, dc=com	Un niveau	cn=Employé1	Recherche plus rapide
2	dc=ExempleSociété,dc=com	Sous-arborescence	cn=Employé1	Recherche plus longue

Lier à un serveur LDAP

L'ASA utilise le nom de domaine (DN) de connexion et le mot de passe de connexion pour établir la confiance (liaison) avec un serveur LDAP. Lors d'une opération en lecture seule Microsoft Active Directory (comme l'authentification, l'autorisation ou la recherche de groupe), l'ASA peut se lier à l'aide d'un DN de connexion avec moins de privilèges. Par exemple, le DN de connexion peut être un utilisateur dont la désignation AD « Membre de » fait partie des utilisateurs de domaine. Pour les opérations de gestion des mots de passe VPN, le nom de domaine de connexion a besoin de privilèges élevés et doit faire partie du groupe AD des opérateurs de compte.

Voici un exemple de DN de connexion :

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

L'ASA prend en charge les méthodes d'authentification suivantes :

- Authentification LDAP simple avec un mot de passe non chiffré sur le port 389

- LDAP sécurisé (LDAP-S) sur le port 636
- Couche d'authentification et de sécurité simple (SASL) MD5
- SASL Kerberos

L'ASA ne prend pas en charge l'authentification anonyme.



Remarque En tant que client LDAP, l'ASA ne prend pas en charge la transmission de liaisons ou de demandes anonymes.

Cartes d'attribut LDAP

L'ASA peut utiliser un répertoire LDAP pour authentifier les utilisateurs pour :

- Les utilisateurs VPN d'accès à distance
- Les sessions d'accès au réseau du pare-feu/de mandataire direct
- La définition des autorisations de politique (également appelées attributs d'autorisation), telles que les ACL, les listes de signets, les paramètres DNS ou WINS et les minuteries de session.
- La définition des attributs clés dans une stratégie de groupe locale

L'ASA utilise des cartes d'attributs LDAP pour traduire les attributs des utilisateurs LDAP natifs en attributs ASA. Vous pouvez lier ces cartes d'attributs aux serveurs LDAP ou les supprimer. Vous pouvez également afficher ou effacer les cartes d'attributs.

La carte d'attributs LDAP ne prend pas en charge les attributs à valeurs multiples. Par exemple, si un utilisateur est membre de plusieurs groupes AD et que la carte d'attributs LDAP correspond à plusieurs groupes, la valeur choisie est basée sur l'ordre alphabétique des entrées correspondantes.

Pour utiliser correctement les fonctionnalités de mappage d'attributs, vous devez comprendre les noms et les valeurs des attributs LDAP, ainsi que les noms et les valeurs des attributs définis par l'utilisateur.

Les noms des attributs LDAP fréquemment mappés et le type d'attributs définis par l'utilisateur auxquels ils sont généralement mappés sont les suivants :

- IETF-Radius-Class (Group_Policy dans ASA version 8.2 et ultérieure) : définit la stratégie de groupe en fonction de la valeur d'attribut du service répertoire ou du groupe d'utilisateurs (par exemple, Microsoft Active Directory memberOf). L'attribut de stratégie de groupe a remplacé l'attribut IETF-Radius-Class par ASDM version 6.2/ASA version 8.2 ou ultérieure.
- IETF-Radius-Filter-Id : applique une liste de contrôle d'accès ou une ACL aux clients VPN, IPsec et SSL.
- IETF-Radius-Framed-IP-Address : attribue une adresse IP statique à un client d'accès à distance VPN, IPsec et SSL.
- Banner1 : affiche une bannière de texte lorsque l'utilisateur d'accès à distance VPN se connecte.
- Tunneling-Protocols : autorise ou refuse la session d'accès à distance VPN en fonction du type d'accès.

Remarque Une seule carte d'attributs LDAP peut contenir un ou plusieurs attributs. Vous ne pouvez mapper qu'un seul attribut LDAP à partir d'un serveur LDAP donné.

Lignes directrices relatives aux serveurs LDAP pour AAA

Cette section inclut des lignes directrices et des limites que vous devez vérifier avant de configurer les serveurs LDAP pour l'AAA.

IPv6

Le serveur AAA peut utiliser une adresse IPv4 ou IPv6.

Directives supplémentaires

- Le DN configuré sur l'ASA pour accéder à un serveur de répertoire Sun doit pouvoir accéder à la politique de mot de passe par défaut sur ce serveur. Nous vous conseillons d'utiliser l'administrateur de répertoire ou un utilisateur disposant des privilèges d'administrateur de répertoire, comme DN. Vous pouvez également placer une ACL sur la politique de mot de passe par défaut.
- Vous devez configurer LDAP sur SSL pour activer la gestion des mots de passe avec les serveurs Microsoft Active Directory et Sun.
- L'ASA ne prend pas en charge la gestion des mots de passe avec Novell, OpenLDAP et les autres serveurs de répertoire LDAPv3.
- À partir de la version 7.1(x), l'ASA effectue l'authentification et l'autorisation à l'aide du schéma LDAP natif, et le schéma Cisco n'est plus nécessaire.
- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 4 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple.
- Lorsqu'un utilisateur se connecte, les serveurs LDAP sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde. Si tous les serveurs du groupe sont indisponibles, l'ASA essaie la base de données locale si vous l'avez configurée comme méthode de secours (authentification et autorisation de gestion uniquement). Si vous n'avez pas de méthode de secours, l'ASA continue d'essayer les serveurs LDAP.

Configurer les serveurs LDAP pour AAA

Cette section décrit comment configurer les serveurs LDAP pour AAA.

Procédure

Étape 1 Configurez les cartes d'attributs LDAP. Consultez Configurer les cartes d'attribut LDAP, à la page 1250.

Étape 2 Ajoutez un groupe de serveurs LDAP. Consultez Configurer les groupes de serveurs LDAP, à la page 1252.

Étape 3 (Facultatif) Configurez l'autorisation à partir d'un serveur LDAP distinct du mécanisme d'authentification. Consultez Configurer l'autorisation avec LDAP pour le VPN, à la page 1254.

Configurer les cartes d'attribut LDAP

Pour configurer les cartes d'attributs LDAP, procédez comme suit :

Procédure

Étape 1 Créez un tableau de cartes d'attributs LDAP non rempli.

ldap-attribute-map *map-name*

Exemple :

```
ciscoasa(config)# ldap-attribute-map att_map_1
```

Étape 2 Mappez le service de nom d'attribut défini par l'utilisateur avec l'attribut Cisco.

map-name *user-attribute-name Cisco-attribute-name*

Exemple :

```
ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class
```

Étape 3 Mappez le service de valeur de carte définie par l'utilisateur avec la valeur de l'attribut définie par l'utilisateur et la valeur de l'attribut Cisco.

map-value *user-attribute-name Cisco-attribute-name*

Exemple :

```
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1
```

Étape 4 Identifiez le serveur et le groupe de serveurs AAA auquel il appartient.

aaa-server *server_group* [*interface_name*] **host** *server_ip*

Exemple :

```
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4
```

Étape 5 Liez la carte d'attributs au serveur LDAP.

ldap-attribute-map *map-name*

Exemple :

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1
```

Exemples

L'exemple suivant montre comment limiter les sessions de gestion à l'ASA en fonction d'un attribut LDAP appelé accessType. L'attribut accessType peut avoir l'une des valeurs suivantes :

- VPN
- admin
- centre d'assistance

L'exemple suivant montre comment chaque valeur est mappée à l'un des attributs IETF-Radius-Service-Type valides que l'ASA prend en charge : remote-access (Service-Type 5) Outbound, admin (Service-Type 6) Administrative et nas-prompt (Service-Type 7) NAS Prompt.

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

L'exemple suivant montre comment afficher la liste complète des noms d'attributs LDAP de Cisco :

```
ciscoasa(config)# ldap attribute-map att_map_1
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
  Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
 :
 :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

Configurer les groupes de serveurs LDAP

Pour créer et configurer un groupe de serveurs LDAP, puis ajouter un serveur LDAP à ce groupe, procédez comme suit :

Avant de commencer

Vous devez ajouter une mise en correspondance d'attributs avant de pouvoir ajouter un serveur LDAP à un groupe de serveurs LDAP.

Procédure

Étape 1 Identifiez le nom du groupe de serveurs et le protocole.

aaa-server *server_tag* **protocol ldap**

Exemple :

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

Lorsque vous saisissez la commande **aaa-server protocol**, vous passez en mode de configuration du groupe aaa-server.

Étape 2 Précisez le nombre maximum de transactions AAA échouées avec un serveur LDAP du groupe avant d'essayer le serveur suivant.

max-failed-attempts *number*

Exemple :

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

L'argument *number* peut aller de 1 à 5. La valeur par défaut est de 3.

Si vous avez configuré une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement) afin de configurer le mécanisme de secours, et que tous les serveurs du groupe ne répondent pas ou que leurs réponses ne sont pas valides, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la commande **reactivation-mode** à l'étape suivante.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

Étape 3 Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

Exemple :

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

Le mot clé **depletion** réactive les serveurs défaillants uniquement après que tous les serveurs du groupe sont inactifs.

La paire mot clé-argument **deadtime** *minutes* spécifie le temps en minutes, entre 0 et 1 440, qui s'écoule entre la désactivation du dernier serveur du groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort. La valeur par défaut est 10 minutes.

Le mot clé **timed** réactive les serveurs défaillants après 30 secondes de temps d'arrêt.

Étape 4 Identifiez le serveur LDAP et le groupe de serveurs AAA auquel il appartient.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

Exemple :

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

Si vous ne spécifiez pas de **(***nom d'interface***)**, l'ASA utilise la de l'interface **interne** par défaut.

Lorsque vous saisissez la commande **aaa-server host**, vous passez en mode de configuration de l'hôte aaa-server. Au besoin, utilisez les commandes du mode de configuration de l'hôte pour configurer davantage le serveur AAA.

Le tableau suivant répertorie les commandes disponibles pour les serveurs LDAP et indique si une nouvelle définition de serveur LDAP a une valeur par défaut ou non. Si aucune valeur par défaut n'est fournie (indiquée par « — »), utilisez la commande pour spécifier la valeur.

Tableau 54 : Commandes et valeurs par défaut du mode d'hôte

Commande	Valeur par défaut	Description
ldap-attribute-map	—	—
ldap-base-dn	—	—
ldap-login-dn	—	—
ldap-login-password	—	—
ldap-naming-attribute	—	—
ldap-over-ssl	636	Si cette option n'est pas définie, l'ASA utilise sAMAccountName pour les demandes LDAP. Que ce soit en utilisant SASL ou du texte brut, vous pouvez sécuriser les communications entre l'ASA et le serveur LDAP avec SSL. Enable SSL (Activer SSL) : nous vous conseillons fortement de sécuriser les communications LDAP avec SSL. Vous pouvez utiliser la commande de sous-mode **reference-identity** pour configurer le nom d'identité de référence que l'ASA utilisera pour valider l'identité du serveur LDAPS (SSL). Une fois configuré, l'ASA valide le serveur aaa-ldap avec les critères de correspondance configurés sous **crypto ca reference-identity** <*name*>. Si aucune correspondance n'a été trouvée dans le nom d'objet ou le SAN du certificat, ou si l'hôte spécifié par l'identité de référence ne se résout pas, la connexion est terminée.

Commande	Valeur par défaut	Description
ldap-scope	—	—
sasl-mechanism	—	—
server-port	389	—
server-type	détection automatique	Si la détection automatique ne parvient pas à déterminer le type de serveur LDAP et que vous savez que le serveur est un serveur Microsoft, Sun ou LDAP générique, vous pouvez configurer manuellement le type de serveur.
ssl-client-certificate	—	Le certificat que l'ASA doit présenter au serveur LDAP en tant que certificat client. Ce certificat est nécessaire si vous configurez le serveur LDAP pour vérifier le certificat client. Vous devez également activer **ldap-over-ssl**. Si vous ne configurez pas de certificat, l'ASA n'en présente pas lorsque le serveur LDAP le demande. Si un serveur LDAP est configuré pour nécessiter un certificat homologue, la session LDAP sécurisée ne se terminera pas, et les demandes d'authentification ou d'autorisation échoueront.
timeout	10secondes	—

Exemple

L'exemple suivant montre comment configurer un groupe de serveurs LDAP nommé watchdogs et ajouter un serveur LDAP au groupe. Comme l'exemple ne définit pas d'intervalle de nouvelle tentative ni le port d'écoute du serveur LDAP, l'ASA utilise les valeurs par défaut pour ces deux paramètres propres au serveur.

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

Configurer l'autorisation avec LDAP pour le VPN

Lorsque l'authentification de l'utilisateur LDAP pour l'accès VPN a réussi, l'ASA interroge le serveur LDAP, qui renvoie les attributs LDAP. Ces attributs comprennent généralement des données d'autorisation qui s'appliquent à la session VPN. L'utilisation de LDAP de cette manière permet d'effectuer l'authentification et l'autorisation en une seule étape.

Il peut arriver que vous ayez besoin de l'autorisation d'un serveur de répertoire LDAP distinct du mécanisme d'authentification. Par exemple, si vous utilisez un serveur SDI ou de certificat pour l'authentification, aucune information d'autorisation n'est renvoyée. Pour les autorisations d'utilisateur dans ce cas, vous pouvez interroger un répertoire LDAP après une authentification réussie, ce qui effectue l'authentification et l'autorisation en deux étapes.

Pour configurer l'autorisation d'utilisateur du VPN à l'aide de LDAP, procédez comme suit.

Procédure

Étape 1 Créez un groupe de tunnels d'accès à distance IPsec nommé remotegrp.

tunnel-group *groupname*

Exemple :

```
ciscoasa(config)# tunnel-group remotegrp
```

Étape 2 Associez le groupe de serveurs et le groupe de tunnels.

tunnel-group *groupname* **general-attributes**

Exemple :

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

Étape 3 Affectez un nouveau groupe de tunnels à un groupe de serveurs AAA précédemment créé pour l'autorisation.

authorization-server-group *group-tag*

Exemple :

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

Exemple

Bien que d'autres commandes et options liées à l'autorisation soient disponibles pour des exigences spécifiques, l'exemple suivant montre les commandes pour activer l'autorisation de l'utilisateur avec LDAP. L'exemple crée ensuite un groupe de tunnels d'accès à distance IPsec nommé remote-1 et affecte ce nouveau groupe de tunnels au groupe de serveurs AAA ldap_dir_1 précédemment créé pour l'autorisation :

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
ciscoasa(config-general)#
```

Après avoir terminé ce travail de configuration, vous pouvez configurer des paramètres d'autorisation LDAP supplémentaires tels que un mot de passe de répertoire, un point de départ pour la recherche dans un répertoire et la portée d'une recherche dans le répertoire en saisissant les commandes suivantes :

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
```

```
ciscoasa(config-aaa-server-host)#
```

Supervision des serveurs LDAP pour AAA

Consultez les commandes suivantes pour superviser les serveurs LDAP pour AAA :

- **show aaa-server**

  Cette commande affiche les statistiques du serveur AAA configuré. Utilisez la commande **clear aaa-server statistics** pour effacer les statistiques du serveur AAA.

- **show running-config aaa-server**

  Cette commande montre la configuration en cours d'exécution du serveur AAA. Utilisez la commande **clear configure aaa-server** pour effacer la configuration du serveur AAA.

Historique des serveurs LDAP pour AAA

Tableau 55 : Historique des serveurs AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs LDAP pour AAA	7.0(1)	Les serveurs LDAP décrivent la prise en charge d'AAA et la configuration des serveurs LDAP. Nous avons introduit les commandes suivantes : **username**, **aaa authorization exec authentication-server**, **aaa authentication console LOCAL**, **aaa authorization exec LOCAL**, **service-type, ldap attribute-map**, **aaa-server protocol**, **aaa authentication telnet** | **ssh** | **serial**} **console LOCAL**, **aaa authentication http console LOCAL**, **aaa authentication enable console LOCAL**, **max-failed-attempts**, **reactivation-mode**, **accounting-mode simultaneous**, **aaa-server host**, **authorization-server-group**, **tunnel-group**, **tunnel-group general-attributes**, **map-name**, **map-value**, **ldap-attribute-map**.
Serveurs LDAP avec adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.

Nom de la caractéristique	Versions de plateforme	Description
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les commandes suivantes pour accepter ces nouvelles limites : **aaa-server**, **aaa-server host**.
Authentification LDAPS mutuelle.	9.18(1)	Vous pouvez configurer un certificat client que l'ASA doit présenter au serveur LDAP lorsqu'il demande un certificat pour l'authentification. Cette fonctionnalité s'applique lorsque vous utilisez LDAP sur SSL. Si un serveur LDAP est configuré pour nécessiter un certificat homologue, la session LDAP sécurisée ne se terminera pas, et les demandes d'authentification ou d'autorisation échoueront. Nous avons ajouté la commande suivante : **ssl-client-certificate**.



CHAPITRE 41

Serveurs Kerberos pour AAA

Les rubriques suivantes expliquent comment configurer les serveurs Kerberos utilisés dans l'AAA. Vous pouvez utiliser des serveurs Kerberos pour l'authentification des connexions de gestion, l'accès réseau et l'accès utilisateur VPN.

- Lignes directrices relatives aux serveurs Kerberos pour AAA, à la page 1259
- Configurer les serveurs Kerberos pour AAA, à la page 1259
- Superviser les serveurs Kerberos pour AAA, à la page 1264
- Historique des serveurs Kerberos pour AAA, à la page 1264

Lignes directrices relatives aux serveurs Kerberos pour AAA

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 8 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple. Lorsqu'un utilisateur se connecte, les serveurs sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde.

Configurer les serveurs Kerberos pour AAA

Les rubriques suivantes expliquent comment configurer les groupes de serveurs Kerberos. Vous pouvez ensuite utiliser ces groupes lors de la configuration de l'accès de gestion ou des VPN.

Configurer les groupes de serveurs AAA Kerberos

Si vous souhaitez utiliser un serveur Kerberos pour l'authentification, vous devez d'abord créer au moins un groupe de serveurs Kerberos et ajouter un ou plusieurs serveurs à chaque groupe.

Procédure

Étape 1 Créez le groupe de serveurs AAA Kerberos et passez en mode de configuration aaa-server-group.

aaa-server *server_group_name* **protocol kerberos**

Exemple :

```
ciscoasa(config)# aaa-server watchdog protocol kerberos
```

Étape 2 (Facultatif) Précisez le nombre maximum de transactions AAA échouées avec un serveur AAA du groupe avant d'essayer le serveur suivant.

max-failed-attempts *number*

Exemple :

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

L'argument *number* peut aller de 1 à 5. La valeur par défaut est de 3.

Si vous avez configuré une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement), et que tous les serveurs du groupe ne répondent pas ou que leurs réponses ne sont pas valides, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la commande **reactivation-mode** à l'étape suivante.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

Étape 3 (Facultatif) Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

Exemple :

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

Le mot clé **depletion** réactive les serveurs défaillants uniquement après que tous les serveurs du groupe sont inactifs. Il s'agit du mode par défaut.

La paire mot clé-argument **deadtime** *minutes* spécifie le temps en minutes, entre 0 et 1 440, qui s'écoule entre la désactivation du dernier serveur du groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort. La valeur par défaut est 10 minutes.

Le mot clé **timed** réactive les serveurs défaillants après 30 secondes d'arrêt.

Étape 4 (Facultatif) Activer la validation du centre de distribution des clés Kerberos (KDC)

validate-kdc

Exemple :

```
ciscoasa(config-aaa-server-group)# validate-kdc
```

Pour réaliser l'authentification, vous devez également importer un fichier keytab que vous avez exporté du centre de distribution des clés Kerberos (KDC). En validant le KDC, vous pouvez empêcher une attaque où l'agresseur usurpe le KDC de sorte que les informations d'authentification de l'utilisateur soient authentifiées sur le serveur Kerberos de l'agresseur.

Pour savoir comment charger le fichier keytab, consultez Configurer la validation du centre de distribution des clés Kerberos, à la page 1263.

Exemple

L'exemple suivant crée un groupe de serveurs Kerberos nommé watchdogs, ajoute un serveur et définit le domaine sur EXEMPLE.COM.

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Ajouter des serveurs Kerberos à un groupe de serveurs Kerberos

Avant de pouvoir utiliser un groupe de serveurs Kerberos, vous devez ajouter au moins un serveur Kerberos au groupe.

Procédure

Étape 1 Ajoutez le serveur Kerberos au groupe de serveurs Kerberos.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

Exemple :

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

Si vous ne spécifiez pas d'interface, l'ASA utilise par défaut la de l'interface **interne**.

Vous pouvez utiliser une adresse IPv4 ou IPv6.

Étape 2 Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

timeout *seconds*

Spécifiez l'intervalle du délai d'expiration (1 à 300 secondes) du serveur; la valeur par défaut est de 10 secondes. Pour chaque transaction AAA, l'ASA relance les tentatives de connexion (en fonction de l'intervalle défini dans la commande **retry-interval**) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite spécifiée dans la commande max-failed-attempts dans le groupe de serveurs AAA, le serveur AAA est désactivé et l'ASA commence à envoyer des demandes à un autre serveur AAA s'il est configuré.

Exemple :

```
ciscoasa(config-aaa-server-host)# timeout 15
```

Étape 3 Spécifiez l'intervalle entre les tentatives, qui correspond au temps d'attente du système avant de réessayer une demande de connexion.

retry-interval *seconds*

Vous pouvez spécifier une valeur comprise entre 1 et 10 secondes. La valeur par défaut est 10.

Exemple :

```
ciscoasa(config-aaa-server-host)# retry-interval 6
```

Étape 4 Spécifiez le port du serveur s'il diffère du port Kerberos par défaut, qui est TCP/88. L'ASA communique avec le serveur Kerberos sur ce port.

server-port *port_number*

Exemple :

```
ciscoasa(config-aaa-server-host)# server-port 8888
```

Étape 5 Configurez le domaine Kerberos.

kerberos-realm *name*

Les noms de domaine Kerberos utilisent uniquement des chiffres et des lettres majuscules et peuvent comporter jusqu'à 64 caractères. Le nom doit correspondre à la sortie de la commande Microsoft Windows **set USERDNSDOMAIN** lorsqu'elle est exécutée sur le serveur Active Directory pour le domaine Kerberos. Dans l'exemple suivant, EXEMPLE.COM est le nom de domaine Kerberos :

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

Bien que l'ASA accepte les lettres minuscules dans le nom, il ne convertit pas les lettres minuscules en majuscules. Assurez-vous d'utiliser uniquement des lettres majuscules.

Exemple :

```
ciscoasa(config-asa-server-group)# kerberos-realm EXAMPLE.COM
```

Exemple

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

Configurer la validation du centre de distribution des clés Kerberos

Vous pouvez configurer un groupe de serveurs AAA Kerberos pour authentifier les serveurs du groupe. Pour réaliser l'authentification, vous devez importer un fichier keytab que vous avez exporté du centre de distribution des clés Kerberos (KDC). En validant le KDC, vous pouvez empêcher une attaque où l'agresseur usurpe le KDC de sorte que les informations d'authentification de l'utilisateur soient authentifiées sur le serveur Kerberos de l'agresseur.

Lorsque vous activez la validation KDC, après avoir obtenu le billet d'octroi de billets (TGT) et validé l'utilisateur, le système demande également un billet de service au nom de l'utilisateur pour host/ASA_hostname. Le système valide ensuite le billet de service renvoyé par rapport à la clé secrète du KDC, qui est stockée dans un fichier keytab que vous avez généré à partir du KDC, puis téléchargé sur l'ASA. En cas d'échec de l'authentification KDC, le serveur est considéré comme non fiable et l'utilisateur n'est pas authentifié.

La procédure suivante explique comment réaliser l'authentification KDC.

Avant de commencer

Vous ne pouvez pas utiliser la validation KDC conjointement avec la délégation Kerberos contrainte (KCD). La commande **validate-kdc** sera ignorée si le groupe de serveurs est utilisé pour le KCD.

Procédure

Étape 1 (Sur le KDC.) Créez un compte d'utilisateur dans Microsoft Active Directory pour l'ASA (accédez à **Start (Démarrage)** > **Programs (Programmes)** > **Administrative Tools (Outils administratifs)** > **Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)**). Par exemple, si le nom de domaine complet (FQDN) de l'ASA est asahost.example.com, créez un utilisateur nommé asahost.

Étape 2 (Sur le KDC.) Créez un nom principal de service d'hôte (SPN) pour l'ASA à l'aide du FQDN et du compte d'utilisateur :

```
C:> setspn -A HOST/asahost.example.com asahost
```

Étape 3 (Sur le KDC.) Créez un fichier keytab pour l'ASA (des sauts de ligne ont été ajoutés pour plus de clarté) :

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

Étape 4 (Sur l'ASA.) Importez le fichier keytab (dans cet exemple, new.keytab) dans l'ASA à l'aide de la commande **aaa kerberos import-keytab**.

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab
ftp://ftpserver.example.com/new.keytab imported successfully
```

Étape 5 (Sur l'ASA.) Ajoutez la commande **validate-kdc** à la configuration du groupe de serveurs AAA Kerberos. Le fichier keytab est utilisé uniquement par les groupes de serveurs qui contiennent cette commande.

```
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa(config-aaa-server-group)# validate-kdc
```

Superviser les serveurs Kerberos pour AAA

Vous pouvez utiliser les commandes suivantes pour superviser et effacer les renseignements relatifs à Kerberos.

- **show aaa-server**

  Affiche les statistiques du serveur AAA. Utilisez la commande **clear aaa-server statistics** pour effacer les statistiques du serveur.

- **show running-config aaa-server**

  Affiche les serveurs AAA configurés pour le système. Utilisez la commande **clear configure aaa-server** pour supprimer la configuration du serveur AAA.

- **show aaa kerberos** [**username** *utilisateur*]

  Affiche tous les billets Kerberos ou les billets pour un nom d'utilisateur donné.

- **clear aaa kerberos tickets** [**username** *utilisateur*]

  Efface tous les billets Kerberos ou les billets pour un nom d'utilisateur donné.

- **show aaa kerberos keytab**

  Affiche des renseignements sur le fichier keytab Kerberos.

- **clear aaa kerberos keytab**

  Efface le fichier keytab Kerberos.

Historique des serveurs Kerberos pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs Kerberos	7.0(1)	Prise en charge des serveurs Kerberos pour AAA. Nous avons introduit les commandes suivantes : **aaa-server protocol**, **max-failed-attempts**, **reactivation-mode**, **aaa-server host**, **kerberos-realm**, **server-port**, **clear aaa-server statistics**, **clear configure aaa-server**, **show aaa-server**, **show running-config aaa-server**, **timeout**.
Adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.

Nom de la caractéristique	Versions de plateforme	Description
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les commandes suivantes pour accepter ces nouvelles limites : **aaa-server**, **aaa-server host**.
Authentification du centre de distribution des clés Kerberos (KDC).	9.8(4) et versions provisoires ultérieures jusqu'à 9.14(1)	Vous pouvez importer un fichier keytab à partir d'un centre de distribution de clés (KDC) Kerberos, et le système peut authentifier que le serveur Kerberos n'est pas falsifié avant de l'utiliser pour authentifier les utilisateurs. Pour réaliser l'authentification par KDC, vous devez configurer un nom de principal de service (SPN) **hôte**/*ASA_hostname* sur le KDC Kerberos, puis exporter un fichier keytab pour ce SPN. Vous devez ensuite charger le fichier keytab sur l'ASA et configurer le groupe de serveurs AAA Kerberos pour valider le KDC. Nous avons ajouté les commandes suivantes : **aaa kerberos import-keytab**, **clear aaa kerberos keytab**, **show aaa kerberos keytab**, **validate-kdc**.



CHAPITRE 42

Configurer les serveurs RSA SecurID pour AAA

Les rubriques suivantes expliquent comment configurer les serveurs RSA SecurID utilisés dans l'AAA. Les serveurs RSA SecureID sont également connus sous le nom de serveurs SDI, car SDI est le protocole utilisé pour communiquer avec eux. Vous pouvez utiliser des serveurs RSA SecurID pour l'authentification des connexions de gestion, l'accès réseau et l'accès utilisateur VPN.

- À propos des serveurs RSA SecurID, à la page 1267
- Lignes directrices relatives aux serveurs RSA SecurID pour AAA, à la page 1267
- Configurer les serveurs RSA SecurID pour AAA, à la page 1268
- Superviser les serveurs RSA SecurID pour AAA, à la page 1271
- Historique des serveurs RSA SecurID pour AAA, à la page 1271

À propos des serveurs RSA SecurID

Vous pouvez utiliser des serveurs RSA SecurID directement pour l'authentification, ou indirectement, comme deuxième facteur d'authentification. Dans ce dernier cas, vous devez configurer la relation avec le serveur SecurID entre le serveur SecurID et votre serveur RADIUS, et configurer l'ASA pour utiliser le serveur RADIUS.

Mais, si vous souhaitez vous authentifier directement auprès du serveur SecurID, vous devez créer un groupe de serveurs AAA pour le protocole SDI, qui est le protocole utilisé pour communiquer avec ces serveurs.

Lorsque vous utilisez SDI, vous n'avez qu'à préciser le serveur SecurID principal lorsque vous créez le groupe de serveurs AAA. L'ASA récupérera le fichier sdiconf.rec, qui répertorie toutes les répliques de serveur SecurID, lors de sa première connexion au serveur. L'ASA peut ensuite utiliser ces répliques pour l'authentification si le serveur principal ne répond pas.

En outre, vous devez enregistrer l'ASA en tant qu'agent d'authentification dans le gestionnaire d'authentification RSA. Les tentatives d'authentification échoueront jusqu'à ce que vous enregistriez l'ASA.

Lignes directrices relatives aux serveurs RSA SecurID pour AAA

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 8 groupes de serveurs par contexte en mode multiple.

- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple. Lorsqu'un utilisateur se connecte, les serveurs sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde.

Configurer les serveurs RSA SecurID pour AAA

Les rubriques suivantes expliquent comment configurer les groupes de serveurs RSA SecurID. Vous pouvez ensuite utiliser ces groupes lors de la configuration de l'accès de gestion ou des VPN.

Configurer les groupes de serveurs RSA SecurID pour AAA

Si vous souhaitez utiliser la communication directe avec un serveur RSA SecurID pour l'authentification, vous devez d'abord créer au moins un groupe de serveurs SDI et ajouter un ou plusieurs serveurs à chaque groupe. Si vous utilisez le serveur SecurID dans une relation mandataire avec un serveur RADIUS, il n'est pas nécessaire de configurer un groupe de serveurs AAA SDI sur l'ASA.

Procédure

Étape 1 Créez le groupe de serveurs AAA SDI et passez en mode de configuration aaa-server-group.

aaa-server *server_group_name* **protocol sdi**

Exemple :

```
ciscoasa(config)# aaa-server watchdog protocol sdi
```

Étape 2 (Facultatif) Précisez le nombre maximum de transactions AAA échouées avec un serveur AAA du groupe avant d'essayer le serveur suivant.

max-failed-attempts *number*

Exemple :

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

L'argument *number* peut aller de 1 à 5. La valeur par défaut est de 3.

Si vous avez configuré une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement), et que tous les serveurs du groupe ne répondent pas ou que leurs réponses ne sont pas valides, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la commande **reactivation-mode** à l'étape suivante.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

Étape 3 (Facultatif) Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

Exemple :

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

Le mot clé **depletion** réactive les serveurs défaillants uniquement après que tous les serveurs du groupe sont inactifs. Il s'agit du mode par défaut.

La paire mot clé-argument **deadtime** *minutes* spécifie le temps en minutes, entre 0 et 1 440, qui s'écoule entre la désactivation du dernier serveur du groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort. La valeur par défaut est 10 minutes.

Le mot clé **timed** réactive les serveurs défaillants après 30 secondes d'arrêt.

Ajouter des serveurs RSA SecurID à un groupe de serveurs SDI

Avant de pouvoir utiliser un groupe de serveurs SDI, vous devez ajouter au moins un serveur RSA SecurID au groupe.

Les serveurs d'un groupe de serveurs SDI utilisent le protocole d'authentification et de gestion de serveur (ACE) pour communiquer avec l'ASA.

Procédure

Étape 1 Ajoutez le serveur RSA SecurID au groupe de serveurs SDI.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

Exemple :

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

Si vous ne spécifiez pas d'interface, l'ASA utilise par défaut la de l'interface **interne**.

Vous pouvez utiliser une adresse IPv4 ou IPv6.

Étape 2 Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

timeout *seconds*

Spécifiez l'intervalle du délai d'expiration (1 à 300 secondes) du serveur; la valeur par défaut est de 10 secondes. Pour chaque transaction AAA, l'ASA relance les tentatives de connexion (en fonction de l'intervalle défini dans la commande **retry-interval**) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite spécifiée dans la commande **max-failed-attempts** dans le groupe de serveurs AAA, le serveur AAA est désactivé et l'ASA commence à envoyer des demandes à un autre serveur AAA s'il est configuré.

Exemple :

```
ciscoasa(config-aaa-server-host)# timeout 15
```

Étape 3 Spécifiez l'intervalle entre les tentatives, qui correspond au temps d'attente du système avant de réessayer une demande de connexion.

retry-interval *seconds*

Vous pouvez spécifier une valeur comprise entre 1 et 10 secondes. La valeur par défaut est 10.

Exemple :

```
ciscoasa(config-aaa-server-host)# retry-interval 6
```

Étape 4 Spécifiez le port du serveur s'il diffère du port RSA SecurID par défaut, qui est TCP/5500. L'ASA communique avec le serveur RSA SecurID sur ce port.

server-port *port_number*

Exemple :

```
ciscoasa(config-aaa-server-host)# server-port 5555
```

Importer le fichier secret de nœud SDI

Vous pouvez importer manuellement le fichier secret du nœud généré par le serveur RSA Authentication Manager (SecurID).

Procédure

Étape 1 Exportez le fichier secret du nœud à partir du serveur RSA Authentication Manager. Pour en savoir plus, consultez la documentation de RSA Authentication Manager.

Étape 2 Placez une version décompressée du fichier secret du nœud sur un serveur auquel vous pouvez accéder à partir de l'ASA ou copiez-la sur l'ASA lui-même.

Le serveur doit prendre en charge l'un des protocoles de transfert suivants : FTP, HTTP, HTTPS, SCP, SMB, TFTP.

Étape 3 Importez le fichier secret du nœud.

aaa sdi import-node-secret *filepath rsa_server_address password*

où :

- *filepath* est le chemin complet vers le fichier secret du nœud décompressé qui a été exporté depuis le RSA Authentication Manager. Les fichiers sur le système local peuvent être désignés par disk0:, disk1: ou flash:. Pour les fichiers sur un serveur distant, utilisez la notation d'URL standard, comme ftp://.
- *rsa_server_address* est l'adresse IP ou le nom d'hôte complet du serveur RSA Authentication Manager auquel appartient le secret du nœud.

• *password* est le mot de passe utilisé pour protéger le fichier lorsque vous l'avez exporté.

Exemple :

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret
nodesecret.rec imported successfully
ciscoasa#
```

Superviser les serveurs RSA SecurID pour AAA

Vous pouvez utiliser les commandes suivantes pour superviser et effacer les renseignements relatifs à RSA SecurID.

- **show aaa-server**

  Affiche les statistiques du serveur AAA. Utilisez la commande **clear aaa-server statistics** pour effacer les statistiques du serveur.

- **show running-config aaa-server**

  Affiche les serveurs AAA configurés pour le système. Utilisez la commande **clear configure aaa-server** pour supprimer la configuration du serveur AAA.

- **show aaa sdi node-secrets**

  Affiche les serveurs RSA SecurID qui ont un fichier secret de nœud importé. Utilisez la commande **clear aaa sdi node-secret** pour supprimer un fichier secret de nœud.

Historique des serveurs RSA SecurID pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs SecurID	7.2(1)	Prise en charge des serveurs SecureID pour AAA pour l'authentification de gestion. SecureID était pris en charge dans les versions précédentes pour l'authentification VPN.
Adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.

Nom de la caractéristique	Versions de plateforme	Description
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les commandes suivantes pour accepter ces nouvelles limites : **aaa-server**, **aaa-server host**.
Importation manuelle du fichier secret du nœud à partir du gestionnaire d'authentification RSA pour les groupes de serveurs AAA SDI.	9.15(1)	Vous pouvez importer le fichier secret du nœud que vous exportez à partir du gestionnaire d'authentification RSA pour l'utiliser avec les groupes de serveurs AAA SDI. Nous avons ajouté les commandes suivantes : **aaa sdi import-node-secret**, **clear aaa sdi node-secret**, **show aaa sdi node-secrets**.



PARTIE VII

Administration système

- Accès de gestion, à la page 1275
- Logiciels et configurations, à la page 1331
- Automatisation de la réponse pour les événements système, à la page 1377
- Tests et dépannage, à la page 1391



CHAPITRE 43

Accès de gestion

Ce chapitre décrit comment accéder à l'ASA pour la gestion de systèmes par le biais de Telnet, SSH et HTTPS (à l'aide d'ASDM), authentifier et autoriser les utilisateurs, et créer des bannières de connexion.

- Configurer l'accès de gestion à distance, à la page 1275
- Configurer AAA pour les administrateurs système, à la page 1296
- Accès au moniteur, à la page 1318
- Historique de l'accès de gestion, à la page 1321

Configurer l'accès de gestion à distance

Cette section décrit comment configurer l'accès ASA pour ASDM, Telnet ou SSH, et d'autres paramètres de gestion tels qu'une bannière de connexion.

Configurer l'accès SSH

Lignes directrices relatives à SSH

- Pour accéder à l'interface ASA pour l'accès SSH, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès SSH conformément à cette section.
- L'accès SSH à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte SSH est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe. La seule exception à cette règle est une connexion VPN (uniquement prise en charge par la pile ASA SSH). Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 1289.
- L'ASA permet un maximum de cinq connexions SSH simultanées par contexte/mode unique, avec un maximum de 100 connexions réparties entre tous les contextes. Cependant, comme les commandes de configuration peuvent obtenir des verrouillages sur les ressources en cours de modification, vous devez apporter des modifications à une session SSH à la fois pour vous assurer que toutes les modifications sont appliquées correctement.
- Par défaut, l'ASA utilise la pile CiscoSSH, qui est basée sur OpenSSH. Vous pouvez choisir d'activer à la place la pile ASA SSH propriétaire. CiscoSSH prend en charge :
  - Conformité FIPS

- Mises à jour régulières, y compris les mises à jour de Cisco et de la communauté de code source libre.

Notez que la pile CiscoSSH ne prend pas en charge :

- SSH vers une interface différente sur VPN (accès de gestion)
- Paire de clés EDDSA
- Paire de clés RSA en mode FIPS

Si vous avez besoin de ces fonctionnalités, vous devez utiliser la pile SSH ASA.

- Pour utiliser la commande **copy** de l'ASA afin de copier un fichier vers ou depuis un serveur SCP, vous devez :
  - (Pile CiscoSSH uniquement) Activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP à l'aide de la commande **ssh**.
  - Générer une paire de clés (pour les ASA physiques uniquement) à l'aide de la commande **crypto key generate**.
- Le nom d'utilisateur SSH par défaut n'est plus pris en charge. Vous ne pouvez plus vous connecter à l'ASA à l'aide de SSH avec le nom d'utilisateur **pix** ou **asa** et le mot de passe de connexion. Pour utiliser SSH, vous devez configurer l'authentification AAA à l'aide de la commande **aaa authentication ssh console LOCAL**; puis définissez un utilisateur local en saisissant la commande **username**. Si vous souhaitez utiliser un serveur AAA pour l'authentification au lieu de la base de données locale, nous vous conseillons de configurer également l'authentification locale comme méthode de sauvegarde.
- Seule la version 2 du protocole SSH est prise en charge.

Pour configurer l'accès SSH à l'ASA, activez le serveur SSH et identifiez les adresses IP autorisées. Pour authentifier les utilisateurs, vous pouvez utiliser les méthodes suivantes :

- Nom d'utilisateur et mot de passe utilisant la base de données locale ou un serveur AAA.
- Nom d'utilisateur et clé publique utilisant la base de données locale.

Activer le serveur SSH

Activez le serveur SSH et spécifiez les adresses IP autorisées à se connecter. Vous pouvez également configurer d'autres paramètres du serveur SSH.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.

Procédure

Étape 1 (Facultatif) Utilisez la pile ASA SSH au lieu de la pile CiscoSSH par défaut.

no ssh stack ciscossh

Pour revenir à la pile CiscoSSH, utilisez **ssh stack ciscossh**.

En mode de contexte multiple, utilisez cette commande dans l'espace d'exécution du système. Pour passer du contexte à la configuration système, saisissez **changeto system**.

Étape 2 Identifiez les adresses IP à partir lesquelles l'ASA accepte les connexions pour chaque adresse ou sous-réseau, et l'interface sur laquelle vous pouvez utiliser SSH.

ssh *source_IP_address mask source_interface*

- *source_interface* : spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 1289), spécifiez l'interface BVI nommée.

Contrairement à Telnet, vous pouvez utiliser SSH sur l'interface de niveau de sécurité le plus bas.

Exemple :

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

Étape 3 (Facultatif) Définissez la durée d'inactivité d'une session SSH avant que l'ASA ne déconnecte la session.

ssh timeout *minutes*

Exemple :

```
ciscoasa(config)# ssh timeout 30
```

Définissez le délai entre une et 60 minutes. La valeur par défaut est 5 minutes. La durée par défaut est trop courte dans la plupart des cas et doit être augmentée jusqu'à ce que tous les tests et dépannages de pré-production soient terminés.

Étape 4 (Facultatif) Activez le serveur Secure Copy (SCP)

ssh scopy enable

Le serveur SCP ne prend pas en charge les répertoires. L'absence de prise en charge des répertoires limite l'accès des clients à distance aux fichiers internes de l'ASA.

Le serveur SCP ne prend pas en charge les bannières ni les caractères génériques.

Étape 5 (Facultatif) Configurez les algorithmes de chiffrement SSH :

ssh cipher encryption {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_encryption_ciphers*}

Exemple :

```
ciscoasa(config)# ssh cipher encryption custom 3des-cbc:aes128-cbc:aes192-cbc
```

La valeur par défaut est **medium**. Les chiffrements sont utilisés dans l'ordre dans lequel ils sont répertoriés. Pour les listes prédéfinies, ils sont répertoriés du plus haut au plus bas niveau de sécurité.

- Le mot clé **all** spécifie l'utilisation de tous les chiffrements : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes192-ctr aes256-ctr
- Le mot clé **custom** spécifie une chaîne de configuration de chiffrement personnalisée, séparée par des deux-points.

- Le mot clé **fips** spécifie uniquement les chiffrements conformes à la norme FIPS : aes128-cbc aes256-cbc
- Le mot clé **high** spécifie uniquement les chiffrements de force élevée : aes256-cbc aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr
- Le mot clé **low** spécifie les chiffrements de force faible, moyenne et élevée : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- Le mot clé **medium** spécifie les chiffrements de force moyenne et élevée (par défaut) : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

Étape 6 (Facultatif) Configurez les algorithmes d'intégrité de chiffrement SSH :

ssh cipher integrity {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_integrity_ciphers*}

Exemple :

```
ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5
```

La valeur par défaut est **high**.

- Le mot clé **all** spécifie l'utilisation de tous les chiffrements : hmac-sha1 hmac-sha1-96 (obsolète) hmac-md5 (obsolète) hmac-md5-96 (obsolète) hmac-sha2-256
- Le mot clé **custom** spécifie une chaîne de configuration de chiffrement personnalisée, séparée par des deux-points.
- Le mot clé **fips** spécifie uniquement les chiffrements conformes à la norme FIPS : hmac-sha1 hmac-sha2-256
- Le mot clé **high** spécifie uniquement les chiffrements de force élevée (par défaut) : hmac-sha2-256
- Le mot clé **low** spécifie les chiffrements de force faible, moyenne et élevée : hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-sha2-256
- Le mot clé **medium** spécifie les chiffrements de force moyenne et élevée : hmac-sha1 hmac-sha1-96 (obsolète) hmac-sha2-256

Étape 7 (Facultatif) (Contexte d'administration uniquement) Définissez le mode d'échange de clés Diffie-Hellman (DH) :

ssh key-exchange group {**curve25519-sha256** | **dh-group14-sha1** | **dh-group14-sha256** | **ecdh-sha2-nistp256**}

Exemple :

```
ciscoasa(config)# ssh key-exchange group dh-group14-sha1
```

La valeur par défaut est **dh-group14-sha256**.

L'échange de clés DH fournit un secret partagé qui ne peut être déterminé par aucune des parties à elles seules. L'échange de clé est combiné à une signature et à la clé de l'hôte pour authentifier l'hôte. Cette méthode d'échange de clés fournit une authentification explicite du serveur. Pour en savoir plus sur l'utilisation des

méthodes d'échange de clés DH, consultez la RFC 4253. Vous ne pouvez définir l'échange de clés que dans le contexte d'administration; cette valeur est utilisée par tous les contextes.

Exemples

L'exemple suivant montre une session SCP vers l'ASA. À partir d'un client sur l'hôte externe, effectuez un transfert de fichiers SCP. Par exemple, dans Linux, saisissez la commande suivante :

scp -v -pw *password* [*path*/]*source_filename*
*username@asa_address***:** {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

L'option **-v** correspond à verbose (détaillé), et si **-pw** n'est pas spécifié, vous serez invité à saisir un mot de passe.

Configurer SSH pour l'accès par mot de passe

Configurez l'authentification SSH à l'aide d'un nom d'utilisateur et d'un mot de passe.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.

Procédure

Étape 1 Générez une paire de clés, requise pour SSH (pour les ASA physiques uniquement).

Pour l'ASA virtuel, les paires de clés sont automatiquement créées après le déploiement.

a) Générez la paire de clés.

crypto key generate {**eddsa edwards-curve ed25519** | **ecdsa elliptic-curve** *size* |**rsa modulus** *size*}

Exemple :

```
ciscoasa(config)# crypto key generate ecdsa elliptic-curve 521
```

- **eddsa edwards-curve ed25519** : la taille de clé est de 256 bits. Non pris en charge avec la pile CiscoSSH.
- **ecdsa elliptic-curve** *size* : la taille en bits est de 256, 384 ou 521.
- **rsa modulus** *size* : la taille en bits est de 2048, 3072 ou 4096.

Plus la taille de clé que vous spécifiez est grande, plus la génération d'une paire de clés prend du temps. SSH essaie les clés dans l'ordre suivant : EdDSA, ECDSA, puis RSA. Affichez les clés à l'aide de la commande **show crypto key mypubkey** {**eddsa** | **ecdsa** | **rsa**}. Les clés utilisées par SSH sont appelées <Default-*type*-Key>.

b) (Facultatif) Si vous ne souhaitez pas utiliser l'ordre de clés par défaut (EdDSA, ECDSA, puis RSA), identifiez la paire de clés que vous souhaitez utiliser.

ssh key-exchange hostkey {**rsa** | **eddsa** | **ecdsa**}

Si vous choisissez RSA, vous devez utiliser une taille de clé de 2048 ou plus. Pour des raisons de compatibilité de mise à niveau, les clés plus petites ne sont prises en charge que lorsque vous utilisez l'ordre de clés par défaut.

Exemple :

```
ciscoasa(config)# ssh key-exchange hostkey ecdsa
```

Étape 2 Enregistrez les clés dans la mémoire flash persistante.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Étape 3 Créez un utilisateur dans la base de données locale ou sur un serveur AAA qui peut être utilisé pour l'accès SSH. Consultez la commande suivante pour ajouter un nom d'utilisateur local (conseillé).

username *name* **password** *password* **privilege** *level*

Vous pouvez utiliser l'authentification par clé publique ou l'authentification par mot de passe pour le même utilisateur local. L'authentification par clé publique n'est pas prise en charge par un serveur AAA.

Exemple :

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

Par défaut, le niveau de privilège est 2; entrez un niveau compris entre 0 et 15, où 15 a tous les privilèges.

Étape 4 Activez l'authentification du serveur local ou AAA pour l'accès SSH.

aaa authentication ssh console {**LOCAL** | *server_group* [**LOCAL**]}

Cette commande n'affecte pas l'authentification par clé publique locale pour les noms d'utilisateur pour lesquels la commande **ssh authentication** est définie. L'ASA utilise implicitement la base de données locale pour l'authentification par clé publique. Cette commande n'affecte que les noms d'utilisateur locaux avec mots de passe. Si vous souhaitez autoriser l'authentification par clé publique ou l'utilisation du mot de passe par un utilisateur local, vous devez configurer explicitement l'authentification locale à l'aide de cette commande pour autoriser l'accès par mot de passe.

Exemple :

```
ciscoasa(config)# aaa authentication ssh console LOCAL
```

Configurer SSH pour l'accès par clé publique

Configurez l'authentification SSH à l'aide d'une clé publique.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.

Procédure

Étape 1 Générez une paire de clés, requise pour SSH (pour les ASA physiques uniquement).

Pour l'ASA virtuel, les paires de clés sont automatiquement créées après le déploiement.

a) Générez la paire de clés.

crypto key generate {**eddsa edwards-curve ed25519** | **ecdsa elliptic-curve** *size* |**rsa modulus** *size*}

Exemple :

```
ciscoasa(config)# crypto key generate ecdsa elliptic-curve 521
```

- **eddsa edwards-curve ed25519** : la taille de clé est de 256 bits. Non pris en charge avec la pile CiscoSSH.
- **ecdsa elliptic-curve** *size* : la taille en bits est de 256, 384 ou 521.
- **rsa modulus** *size* : la taille en bits est de 2048, 3072 ou 4096.

Plus la taille de clé que vous spécifiez est grande, plus la génération d'une paire de clés prend du temps. SSH essaie les clés dans l'ordre suivant : EdDSA, ECDSA, puis RSA. Affichez les clés à l'aide de la commande **show crypto key mypubkey** {**eddsa** | **ecdsa** | **rsa**}. Les clés utilisées par SSH sont appelées <Default-*type*-Key>.

b) (Facultatif) Si vous ne souhaitez pas utiliser l'ordre de clés par défaut (EdDSA, ECDSA, puis RSA), identifiez la paire de clés que vous souhaitez utiliser.

ssh key-exchange hostkey {**rsa** | **eddsa** | **ecdsa**}

Si vous choisissez RSA, vous devez utiliser une taille de clé de 2048 ou plus. Pour des raisons de compatibilité de mise à niveau, les clés plus petites ne sont prises en charge que lorsque vous utilisez l'ordre de clés par défaut.

Exemple :

```
ciscoasa(config)# ssh key-exchange hostkey ecdsa
```

Étape 2 Enregistrez les clés dans la mémoire flash persistante.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Étape 3 Créez un utilisateur dans la base de données locale qui peut être utilisé pour l'accès SSH.

username *nom* [**password** *mot de passe*] **privilege** *niveau*

Exemple :

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

Par défaut, le niveau de privilège est 2; entrez un niveau compris entre 0 et 15, où 15 a tous les privilèges. Vous pouvez créer un utilisateur sans mot de passe si vous souhaitez forcer l'utilisateur à utiliser l'authentification par clé publique (**ssh authentication**) au lieu de l'authentification par mot de passe. Si vous configurez l'authentification par clé publique ainsi qu'un mot de passe dans la commande **username**, l'utilisateur peut se connecter en utilisant l'une ou l'autre des méthodes si vous configurez explicitement l'authentification AAA dans Configurer SSH pour l'accès par mot de passe, à la page 1279. **Remarque :** N'utilisez pas la commande **username** l'option **nopassword**; l'option **nopassword** permet de saisir *n'importe quel* mot de passe, et non pas aucun mot de passe.

Étape 4 Autorisez l'authentification par clé publique pour un utilisateur au lieu de/ou l'authentification par mot de passe, et saisissez la clé publique sur l'ASA :

username *nom* **attributes**

ssh authentication {**pkf** | **publickey** *key*}

Exemple :

```
ciscoasa(config)# username admin attributes
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
```

Pour un **username** local, vous pouvez activer l'authentification par clé publique au lieu de l'authentification par mot de passe. Vous pouvez générer une paire de clés publiques/privées à l'aide de n'importe quel logiciel de génération de clés SSH (comme ssh keygen) qui peut générer des clés brutes ssh-rsa, ssh-ed25519 ou ecdsa-sha2-nistp (sans certificats). Saisissez la clé publique sur l'ASA. Le client SSH utilise ensuite la clé privée (et la phrase secrète que vous avez utilisée pour créer la paire de clés) pour se connecter à l'ASA.

Pour une clé **pkf**, vous êtes invité à coller une clé au format PKF, jusqu'à 4096 bits. Utilisez ce format pour les clés trop importantes pour les coller en ligne au format base64. Par exemple, vous pouvez générer une clé de 4096 bits à l'aide de ssh keygen, puis la convertir en PKF, et utiliser le mot clé **pkf** pour être invité à saisir la clé. **Remarque :** Vous pouvez utiliser l'option **pkf** avec le basculement, mais la clé PKF n'est pas automatiquement répliquée sur le système de secours. Vous devez saisir la commande **write standby** pour synchroniser la clé PKF.

Pour la valeur **publickey** *key*, la clé est une clé publique codée en Base64. Vous pouvez générer la clé à l'aide de n'importe quel logiciel de génération de clés SSH (comme ssh keygen) qui peut générer des clés brutes ssh-rsa, ssh-ed25519 ou ecdsa-sha2-nistp (sans certificats).

Exemples

L'exemple suivant montre comment s'authentifier à l'aide d'une clé au format PKF :

```
ciscoasa(config)# crypto key generate rsa modulus 4096
ciscoasa(config)# write memory
ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# username exampleuser1 attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config)#
```

L'exemple suivant génère une clé partagée pour SSH sur un système Linux ou Macintosh et l'importe dans l'ASA :

1. Générez les clés publiques et privées RSA pour 4 096 bits sur votre ordinateur :

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

2. Convertissez la clé au format PKF :

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by john@jcrichton-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. Copiez la clé dans votre presse-papiers.
4. Dans ASDM, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, sélectionnez le nom d'utilisateur, puis cliquez sur **Edit** (Modifier). Cliquez sur **Public Key Using PKF** (Clé publique utilisant PKF) et collez la clé dans la fenêtre :
5. Vérifiez que l'utilisateur peut se connecter par SSH à l'ASA. Pour le mot de passe, saisissez le mot de passe de la clé SSH que vous avez spécifié lors de la création de la paire de clés.

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

La boîte de dialogue suivante s'affiche pour que vous puissiez saisir votre phrase secrète :



Pendant ce temps, dans la session de terminal :

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

Configurer l'accès Telnet

Pour identifier les adresses IP clients autorisées à se connecter à l'ASA à l'aide de Telnet, procédez comme suit. Consultez les consignes suivantes :

- Pour accéder à l'interface ASA pour l'accès Telnet, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès Telnet conformément à cette section.
- L'accès Telnet à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte Telnet est situé sur l'interface externe, vous ne pouvez initier une connexion Telnet que directement à l'interface externe. La seule exception à cette règle est une connexion VPN. Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 1289.
- Vous ne pouvez pas utiliser Telnet sur l'interface de sécurité la plus basse, sauf si vous utilisez Telnet dans un tunnel VPN.
- L'ASA permet un maximum de cinq connexions Telnet simultanées par contexte/mode unique, avec un maximum de 100 connexions réparties entre tous les contextes.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.
- Pour accéder à l'interface de ligne de commande d'ASA à l'aide de Telnet, saisissez le mot de passe de connexion défini par la commande **password**. Vous devez définir manuellement le mot de passe avant d'utiliser Telnet.

Procédure

Étape 1 Identifiez les adresses IP à partir desquelles l'ASA accepte les connexions pour chaque adresse ou sous-réseau sur l'interface spécifiée.

telnet *source_IP_address mask source_interface*

- *source_interface* : spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 1289), spécifiez l'interface BVI nommée.

S'il n'existe qu'une seule interface, vous pouvez configurer Telnet pour accéder à cette interface tant que son niveau de sécurité est de 100.

Exemple :

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

Étape 2 Définissez la durée d'inactivité d'une session Telnet avant que l'ASA ne déconnecte la session.

telnet timeout *minutes*

Exemple :

```
ciscoasa(config)#  telnet timeout 30
```

Définissez le délai entre une et 1 440 minutes. La valeur par défaut est 5 minutes. La durée par défaut est trop courte dans la plupart des cas et devrait être augmentée jusqu'à ce que tous les tests de pré-production et le dépannage soient terminés.

Exemples

L'exemple suivant montre comment autoriser un hôte sur l'interface interne avec l'adresse 192.168.1.2 à accéder à l'ASA :

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

L'exemple suivant montre comment autoriser tous les utilisateurs du réseau 192.168.3.0 à accéder à l'ASA sur l'interface interne :

```
ciscoasa(config)# telnet 192.168.3.0. 255.255.255.255 inside
```

Configurer l'accès HTTPS pour ASDM, autres clients

Pour utiliser ASDM ou d'autres clients HTTPS tels que CSM, vous devez activer le serveur HTTPS et autoriser les connexions HTTPS à l'ASA. L'accès HTTPS est activé dans le cadre de la configuration d'usine par défaut. Pour configurer l'accès HTTPS, procédez comme suit. Consultez les consignes suivantes :

- Pour accéder à l'interface ASA pour l'accès HTTPS, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès HTTPS conformément à cette section. Si, toutefois, vous configurez la redirection HTTP pour rediriger automatiquement les connexions HTTP vers HTTPS, vous devez activer un critère d'accès pour autoriser HTTP; sinon, l'interface ne peut pas être à l'écoute du port HTTP.
- L'accès de gestion à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte de gestion est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe. La seule exception à cette règle est une connexion VPN. Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 1289.
- En mode de contexte unique, vous pouvez avoir un maximum de 5 sessions ASDM simultanées. En mode de contexte multiple, vous pouvez avoir un maximum de 5 sessions ASDM simultanées par contexte, avec un maximum de 200 instances ASDM parmi tous les contextes.

  Les sessions ASDM utilisent deux connexions HTTPS: une pour la surveillance qui est toujours présente et une pour apporter des modifications de configuration qui est présente uniquement lorsque vous apportez des modifications. Par exemple, la limite système en mode de contexte multiple de 200 sessions ASDM représente une limite de 400 sessions HTTPS.
- L'ASA permet un maximum de 6 sessions HTTPS non ASDM simultanées en mode de contexte unique ou par contexte, si disponible, avec un maximum de 100 sessions HTTPS parmi tous les contextes.

- Si vous avez activé SSL (**webvpn** > **enable** *interface*) et l'accès HTTPS sur la même interface, vous pouvez accéder à Secure Client (services client sécurisés) à partir de l'adresse **https://***ip_address* et à ASDM à partir de l'adresse **https://***ip_address*/**admin**, tous deux sur le port 443. Si vous activez également **aaa authentication http console**, vous devez alors spécifier un port différent pour l'accès à ASDM.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.

Procédure

Étape 1 Identifiez les adresses IP à partir desquelles l'ASA accepte les connexions HTTPS pour chaque adresse ou sous-réseau sur l'interface spécifiée.

http *source_IP_address mask source_interface*

- *source_interface* : spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 1289), spécifiez l'interface BVI nommée.

Exemple :

```
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

Étape 2 Activez le serveur HTTPS.

http server enable [*port*]

Exemple :

```
ciscoasa(config)# http server enable 444
```

Par défaut, le port est 443. Si vous modifiez le numéro de port, veillez à l'inclure dans l'URL d'accès ASDM. Par exemple, si vous définissez le numéro de port à 444, saisissez l'URL suivante :

https://10.1.1.1:444

Étape 3 Autorisez les clients HTTPS non basés sur le navigateur à accéder aux services HTTPS sur l'ASA. Par défaut, ASDM, CSM et l'API REST sont autorisés.

http server basic-auth-client *user_agent*

- *user_agent* : spécifie la chaîne User-Agent du client dans l'en-tête HTTP de la requête HTTP. Vous pouvez spécifier la chaîne complète ou une chaîne partielle; les chaînes partielles doivent correspondre au début de la chaîne User-Agent. Nous conseillons d'utiliser des chaînes complètes pour une meilleure sécurité. Notez que la chaîne est sensible à la casse.

  Par exemple, **curl** correspondra à la chaîne User-Agent suivante :

  curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

curl ne correspond *pas* à la chaîne User-Agent suivante :

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1
Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

CURL ne correspond *pas* à la chaîne User-Agent suivante :

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

Saisissez chaque chaîne client à l'aide d'une commande distincte.De nombreux clients spécialistes (par exemple, les bibliothèques python, curl et wget) ne prennent pas en charge l'authentification basée sur le jeton Cross-site Request Forgery (CSRF). Vous devez donc autoriser expressément ces clients à utiliser la méthode d'authentification de base de l'ASA. Pour des raisons de sécurité, vous ne devez autoriser que les clients requis.

Exemple :

```
ciscoasa(config)# http server basic-auth-client curl
```

Étape 4 (Facultatif) Définissez les délais de connexion et de session.

http server idle-timeout*minutes*

http server session-timeout*minutes*

http connection idle-timeout*seconds*

- **http server idle-timeout** *minutes* : définissez le délai d'inactivité pour les connexions ASDM, de 1 à 1 440 minutes. La valeur par défaut est 20 minutes. L'ASA déconnecte une connexion ASDM qui est inactive pendant la période définie.
- **http server session-timeout** *minutes* : définissez le session expirée pour les sessions ASDM, de 1 à 1 440 minutes. Ce délai est désactivé par défaut. L'ASA déconnecte une session ASDM qui dépasse la période définie.
- **http connection idle-timeout** *seconds* : définissez le délai d'inactivité pour toutes les connexions HTTPS, y compris ASDM, WebVPN et d'autres clients, de 10 à 86 400 secondes. Ce délai est désactivé par défaut. L'ASA déconnecte une connexion qui est inactive pendant la période définie. Si vous définissez les commandes **http server idle-timeout** et **http connection idle-timeout**, la commande **http connection idle-timeout** prévaut.

Exemple :

```
ciscoasa(config)# http server idle-timeout 30
ciscoasa(config)# http server session-timeout 120
```

Exemples

L'exemple suivant montre comment activer le serveur HTTPS et autoriser un hôte sur l'interface interne avec l'adresse 192.168.1.2 à accéder à ASDM :

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

L'exemple suivant montre comment autoriser tous les utilisateurs du réseau 192.168.3.0/24 à accéder à ASDM sur l'interface interne :

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

Configurer la redirection HTTP pour l'accès ASDM ou le SSL VPN sans client

Vous devez utiliser HTTPS pour vous connecter à l'ASA à l'aide d'ASDM ou du SSL VPN sans client. Pour plus de commodité, vous pouvez rediriger les connexions de gestion HTTP vers HTTPS. Par exemple, en redirigeant HTTP, vous pouvez saisir **http://10.1.8.4/admin/** ou **https://10.1.8.4/admin/** et arriver toujours à la page de lancement d'ASDM à l'adresse HTTPS.

Vous pouvez rediriger le trafic IPv4 et IPv6.

Avant de commencer

Normalement, vous n'avez pas besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Cependant, pour la redirection HTTP, vous devez activer un critère d'accès pour autoriser HTTP; sinon, l'interface ne peut pas être à l'écoute du port HTTP.

Procédure

Activez la redirection HTTP :

http redirect *interface_name* [*port*]

Exemple :

```
ciscoasa(config)# http redirect outside 88
```

Le *port* identifie le port à partir duquel l'interface redirige les connexions HTTP. La valeur par défaut est 80.

Configurer l'accès de gestion sur un tunnel VPN

Si votre tunnel VPN se termine sur une interface, mais que vous souhaitez gérer l'ASA en accédant à une autre interface, vous devez identifier cette interface comme une interface d'accès de gestion. Par exemple, si vous saisissez l'ASA à partir de l'interface externe, cette fonctionnalité vous permet de vous connecter à l'interface interne à l'aide d'ASDM, SSHou Telnet; ou vous pouvez envoyer un message Ping à l'interface interne en entrant à partir de l'interface externe.

Remarque Cette fonctionnalité n'est pas prise en charge pour SSH si vous utilisez la pile CiscoSSH, qui est la valeur par défaut.

Remarque Cette fonctionnalité n'est pas prise en charge pour SNMP. Pour SNMP sur VPN, nous vous recommandons d'activer SNMP sur une interface de boucle avec retour. Vous n'avez pas besoin d'activer la fonctionnalité d'accès de gestion pour utiliser SNMP sur l'interface de boucle avec retour. La boucle avec retour fonctionne également pour SSH.

L'accès VPN à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre accès VPN se trouve sur l'interface externe, vous pouvez uniquement initier une connexion directement à l'interface externe. Vous devez activer le VPN sur l'interface directement accessible de l'ASA et utiliser la résolution de noms pour ne pas avoir à vous souvenir de plusieurs adresses.

L'accès de gestion est disponible par les types de tunnel VPN suivants : clients IPsec, IPsec de site à site, Easy VPN et le SSL VPN Secure Client (services client sécurisés).

Avant de commencer

- Cette fonctionnalité n'est pas prise en charge sur les interfaces de gestion uniquement.
- Lorsque vous utilisez une interface d'accès de gestion et que vous configurez la NAT d'identité, vous devez configurer la NAT avec l'option de recherche de routage. Pour en savoir plus, consultez la section « Accès à la gestion de la NAT et du VPN » dans le chapitre *Exemples de NAT et référence* dans la version appropriée du Guide de configuration de l'interface de ligne de commande du pare-feu ASA.

Procédure

Précisez le nom de l'interface de gestion à laquelle vous souhaitez accéder lorsque vous saisissez l'ASA à partir d'une autre interface.

management-access *management_interface*

Pour les tunnels Easy VPN et Site à site, vous pouvez spécifier une BVI nommée (en mode routé).

Exemple :

```
ciscoasa(config)# management-access inside
```

Configurer l'accès de gestion pour FXOS sur les interfaces de données en mode plateforme Firepower 2100

Si vous souhaitez gérer FXOS sur le Firepower 2100 en mode plateforme à partir d'une interface de données, vous pouvez configurer l'accès SSH, HTTPS et SNMP. Cette fonctionnalité est utile si vous souhaitez gérer le périphérique à distance, mais que vous souhaitez conserver la gestion 1/1, qui est la méthode d'accès native à FXOS, sur un réseau isolé. Si vous activez cette fonctionnalité, vous pouvez continuer à utiliser l'interface de gestion Management 1/1 pour l'accès local uniquement. Cependant, vous ne pouvez pas autoriser l'accès *à distance* depuis ou vers l'interface de gestion Management 1/1 pour FXOS en même temps que l'utilisation de cette fonctionnalité. Cette fonctionnalité nécessite le transfert du trafic vers les interfaces de données ASA

à l'aide d'un chemin interne (valeur par défaut), et vous ne pouvez spécifier qu'une seule passerelle de gestion FXOS.

L'ASA utilise des ports non standard pour l'accès FXOS; le port standard est réservé à l'utilisation par l'ASA sur la même interface. Lorsque l'ASA transfère le trafic vers FXOS, il traduit le port de destination non standard en port FXOS pour chaque protocole (ne modifiez pas le port HTTPS dans FXOS). L'adresse IP de destination du paquet (qui est l'adresse IP de l'interface ASA) est également convertie en une adresse interne pour l'utilisation par FXOS. L'adresse source reste inchangée. Pour renvoyer le trafic, l'ASA utilise sa table de routage de données pour déterminer la bonne interface de sortie. Lorsque vous accédez à l'adresse IP de données ASA pour l'application de gestion, vous devez vous connecter en utilisant un nom d'utilisateur FXOS; les noms d'utilisateur ASA ne s'appliquent qu'à l'accès de gestion ASA.

Vous pouvez également activer l'*initiation* du trafic de gestion FXOS sur les interfaces de données ASA. Cette fonction est requise pour les alertes SNMP ou pour l'accès au serveur NTP et DNS, par exemple. Par défaut, l'initiation du trafic de gestion FXOS est activée pour l'interface externe ASA pour la communication avec les serveurs DNS et NTP (cette fonctionnalité est requise pour la communication avec les licences Smart).

Avant de commencer

- Mode contexte unique seulement.
- Exclut les interfaces de gestion ASA uniquement.
- Vous ne pouvez pas utiliser un tunnel VPN pour l'interface de données ASA et accéder directement à FXOS. Comme solution de contournement pour SSH, vous pouvez faire appel au VPN vers l'ASA, accéder à l'interface de ligne de commande de l'*ASA*, puis utiliser la commande **connect fxos** pour accéder à l'interface de ligne de commande de FXOS. Notez que SSH, HTTPS et SNMPv3 sont/peuvent être chiffrés, de sorte qu'une connexion directe à l'interface de données est sécurisée.
- Assurez-vous que la passerelle FXOS est configurée pour acheminer le trafic vers les interfaces de données ASA (par défaut). Consultez le guide de démarrage pour en savoir plus sur la configuration de la passerelle.

Procédure

Étape 1 Activez la gestion à distance FXOS.

fxos {**https** | **ssh** | **snmp**} **permit** {*ipv4_address netmask* | *ipv6_address/prefix_length*} *interface_name*

Exemple :

```
ciscoasa(config)# fxos https permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos https permit 2001:DB8::34/64 inside
ciscoasa(config)# fxos ssh permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos ssh permit 2001:DB8::34/64 inside
```

Étape 2 (Facultatif) Modifiez le port par défaut pour le service.

fxos {**https** | **ssh** | **snmp**} **port** *port*

Consultez les paramètres par défaut suivants :

- Port HTTPS par défaut : 3443

- Port SNMP par défaut : 3061
- Port SSH par défaut : 3022

Exemple :

```
ciscoasa(config)# fxos https port 6666
ciscoasa(config)# fxos ssh port 7777
```

Étape 3 Permettez à FXOS d'initier des connexions de gestion à partir de l'interface ASA.

ip-client *interface_name*

Par défaut, l'interface externe est activée.

Exemple :

```
ciscoasa(config)# ip-client outside
ciscoasa(config)# ip-client services
```

Étape 4 Connectez-vous à Firewall Chassis Manager sur l'interface de gestion Management 1/1 (par défaut https://192.168.45.45, avec le nom d'utilisateur : **admin** et le mot de passe : **Admin123**).

Étape 5 Cliquez sur l'onglet **Platform Settings** (paramètres de plateforme) et activez **SSH**, **HTTPS** ou **SNMP**.

SSH et HTTPS sont activés par défaut.

Étape 6 Configurez une liste d'accès (**Access List**) dans l'onglet des paramètres de la plateforme (**Platform Settings**) pour autoriser vos adresses de gestion. SSH et HTTPS autorisent uniquement le réseau de gestion Management 1/1 192.168.45.0 par défaut. Vous devez autoriser toutes les adresses que vous avez spécifiées dans la configuration de gestion à distance FXOS (**FXOS Remote Management**) sur l'ASA.

Modifier le délai d'expiration de la console

Le délai d'expiration de la console définit combien de temps une connexion peut rester en mode d'exécution privilégié ou en mode de configuration; une fois le délai d'expiration atteint, la session passe en mode EXEC de l'utilisateur. Par défaut, la session n'expire pas. Ce paramètre n'a pas d'incidence sur la durée de votre connexion au port de console, qui n'expire jamais.

Procédure

Spécifiez le délai d'inactivité en minutes (0 à 60) après quoi la session privilégiée se termine.

console timeout *number*

Exemple :

```
ciscoasa(config)# console timeout 0
```

La valeur d'expiration par défaut est 0, ce qui signifie que la session n'expire pas.

Personnaliser une invite de l'interface de ligne de commande

La possibilité d'ajouter des renseignements à une invite vous permet de voir en un coup d'œil à quel ASA vous êtes connecté lorsque vous avez plusieurs modules. Lors d'un basculement, cette fonctionnalité est utile lorsque les deux ASA ont le même nom d'hôte.

En mode de contexte multiple, vous pouvez afficher l'invite étendue lorsque vous vous connectez à l'espace d'exécution du système ou au contexte d'administration. Dans un contexte de non-administration, vous ne voyez que l'invite par défaut, qui est le nom d'hôte et le nom de contexte.

Par défaut, l'invite affiche le nom d'hôte de l'ASA. En mode de contexte multiple, l'invite affiche également le nom du contexte. Vous pouvez afficher les éléments suivants dans l'invite de l'interface de ligne de commande :

cluster-unit	Affiche le nom de l'unité de grappe. Chaque unité d'une grappe peut avoir un nom unique.
context	(Mode multiple uniquement) Affiche le nom du contexte actuel.
domaine	Affiche le nom de domaine.
hostname	Affiche le nom d'hôte.
priority	Affiche la priorité de basculement comme pri (principal) ou sec (secondaire).
state	Affiche l'état de transmission du trafic ou le rôle de l'unité. Pour le basculement, les valeurs suivantes sont affichées pour le mot clé d'état : • **act** : le basculement est activé et l'unité transmet activement le trafic. • **stby** : le basculement est activé et l'unité ne transmet pas de trafic et est en veille, en panne ou dans un autre état non actif. • **actNoFailover** : le basculement n'est pas activé et l'unité transmet activement le trafic. • **stbyNoFailover** : le basculement n'est pas activé et l'unité ne transmet pas de trafic. Cela pourrait se produire en cas de défaillance d'interface au-dessus du seuil sur l'unité en veille. Pour la mise en grappe, les valeurs du contrôle et des données sont affichées.

Procédure

Personnalisez l'invite de l'interface de ligne de commande en saisissant la commande suivante :

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

Exemple :

```
ciscoasa(config)# prompt hostname context slot state priority
ciscoasa/admin/pri/act(config)#
```

L'ordre dans lequel vous saisissez les mots clés détermine l'ordre des éléments dans l'invite, qui sont séparés par une barre oblique (/).

Configurer une bannière de connexion

Vous pouvez configurer un message pour qu'il s'affiche lorsqu'un utilisateur se connecte à l'ASA, avant qu'un utilisateur ne se connecte ou avant qu'un utilisateur n'entre en mode d'exécution privilégié.

Avant de commencer

- Du point de vue de la sécurité, il est important que votre bannière dissuade les accès non autorisés. N'utilisez pas les mots « bienvenue » ou « s'il vous plaît », car ils semblent inviter des intrus à entrer. La bannière suivante donne le bon ton en cas d'accès non autorisé :

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- Après l'ajout d'une bannière, les sessions Telnet ou SSH à l'ASA peuvent se fermer si :
  - La mémoire système est insuffisante pour traiter les messages sur bannière.
  - Une erreur d'écriture TCP se produit lors de la tentative d'affichage des messages sur bannière.
- Consultez la RFC 2196 pour connaître les lignes directrices relatives aux messages sur bannière.

Procédure

Ajoutez une bannière à afficher à l'un des trois moments suivants : lorsqu'un utilisateur se connecte pour la première fois (message du jour (motd)), lorsqu'un utilisateur se connecte (connexion) et lorsqu'un utilisateur accède au mode d'exécution privilégié (exec).

banner {**exec** | **login** | **motd**} *texte*

Exemple :

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).
```

Lorsqu'un utilisateur se connecte à l'ASA, la bannière message-du-jour s'affiche en premier, suivie de la bannière de connexion et des invites. Une fois que l'utilisateur a bien été connecté à l'ASA, la bannière d'exécution s'affiche.

Pour ajouter plusieurs lignes, précédez chaque ligne par la commande **banner**.

Pour le texte de la bannière :

- Les espaces sont autorisés, mais les onglets ne peuvent pas être saisis à l'aide de l'interface de ligne de commande.
- Il n'y a aucune limite de longueur de bannière autre que celles de la RAM et de la mémoire flash.

- Vous pouvez ajouter de manière dynamique le nom d'hôte ou le nom de domaine de l'ASA en incluant les chaînes **$(hostname)** et **$(domain)**.
- Si vous configurez une bannière dans la configuration système, vous pouvez utiliser ce texte de bannière dans un contexte en utilisant la chaîne **$(system)** dans la configuration du contexte.

Exemples

Les exemples suivants montrent comment ajouter une bannière de message du jour :

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).

ciscoasa(config)# banner motd Contact me at admin@example.com for any issues.
```

Définir un quota de sessions de gestion

Vous pouvez établir un nombre maximum de sessions ASDM, SSH et Telnet simultanées qui sont autorisées sur l'ASA. Si le maximum est atteint, aucune session supplémentaire n'est autorisée et un message de journal système est généré. Pour empêcher un verrouillage du système, le mécanisme de quota de sessions de gestion ne peut pas bloquer une session de console.

Remarque En mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions ASDM, où le maximum est fixe à 5 sessions.

Remarque Si vous définissez également une limite de ressources par contexte pour le nombre maximum de sessions administratives (SSH, etc.), la valeur la plus basse sera utilisée.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez le contexte **changeto context** *name*.

Procédure

Étape 1 Entrez la commande suivante :

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

- **ssh** : définit le nombre maximum de sessions SSH, entre 1 et 5. La valeur par défaut est égale à 5.
- **telnet** : définit le nombre maximum de sessions Telnet, entre 1 et 5. La valeur par défaut est égale à 5.

- **http** : définit le nombre maximum de sessions HTTPS (ASDM), entre 1 et 5. La valeur par défaut est égale à 5.
- **user** : définit le nombre maximum de sessions par utilisateur, entre 1 et 5. La valeur par défaut est égale à 5.
- *number* : définit le nombre de sessions. Lorsqu'il est saisi sans autre mot clé, cet argument définit le nombre agrégé de sessions entre 1 et 15. La valeur par défaut est de 15.

Exemple :

```
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

Étape 2 Affichez les sessions actuellement utilisées.

show quota management-session [**ssh** | **telnet** | **http** | **user**]

Exemple :

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                 Username
1                              SSH                     cisco
2                              TELNET                  cisco
1                              SSH                     cisco1
```

Configurer AAA pour les administrateurs système

Cette section décrit comment configurer l'authentification, l'autorisation de gestion et l'autorisation de commande pour les administrateurs système.

Configurer l'authentification de gestion

Configurez l'authentification pour l'accès à l'interface de ligne de commande et à ASDM.

À propos de l'authentification de gestion

La façon dont vous vous connectez à l'ASA dépend de si vous activez ou non l'authentification.

À propos de l'authentification SSH

Consultez le comportement suivant pour l'accès SSH avec et sans authentification :

- Aucune authentification : SSH n'est pas disponible sans authentification.
- Authentification : lorsque vous activez l'authentification SSH, vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données locale des utilisateurs. Pour l'authentification par clé publique, l'ASA ne prend en charge que la base de données locale. Si vous

configurez l'authentification par clé publique SSH, l'ASA utilise implicitement la base de données locale. Il vous suffit de configurer explicitement l'authentification SSH lorsque vous utilisez un nom d'utilisateur et un mot de passe pour vous connecter. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'authentification Telnet

Consultez le comportement suivant pour l'accès Telnet avec et sans authentification :

- Aucune authentification : si vous n'activez aucune authentification pour Telnet, vous ne saisissez pas de nom d'utilisateur; vous saisissez le mot de passe de connexion (défini avec la commande **password**). Il n'y a pas de mot de passe par défaut, vous devez donc en définir un avant de pouvoir vous connecter à l'ASA via Telnet. Vous accédez au mode EXEC de l'utilisateur.
- Authentification : si vous activez l'authentification Telnet, vous saisissez le nom d'utilisateur et le mot de passe définis sur le serveur AAA ou la base de données des utilisateurs locale. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'authentification ASDM

Consultez le comportement suivant pour l'accès ASDM avec et sans authentification. Vous pouvez également configurer l'authentification par certificat, avec ou sans authentification AAA.

- Aucune authentification : par défaut, vous pouvez vous connecter à ASDM avec un nom d'utilisateur vide et le mot de passe d'activation défini par la commande **enable password**, qui est vide par défaut. Nous vous suggérons de modifier le mot de passe d'activation dès que possible afin qu'il ne reste pas vide; voir Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet, à la page 831. Lorsque vous saisissez la commande **enable** au niveau de l'interface de ligne de commande pour la première fois, vous êtes invité à modifier le mot de passe; ce comportement n'est pas appliqué lorsque vous vous connectez à ASDM. Notez que si vous saisissez un nom d'utilisateur et un mot de passe à l'écran de connexion (au lieu de laisser le nom d'utilisateur vide), ASDM vérifie la base de données locale à la recherche d'une correspondance.
- Authentification par certificat : (mode unique et routé uniquement) Vous pouvez exiger que l'utilisateur ait un certificat valide. Saisissez le nom d'utilisateur et le mot de passe du certificat pour que l'ASA valide le certificat par rapport au point de confiance PKI.
- Authentification AAA : lorsque vous activez l'authentification ASDM (HTTPS), vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données locale des utilisateurs. Vous ne pouvez plus utiliser ASDM avec un nom d'utilisateur vide et le mot de passe d'activation.
- Authentification AAA plus authentification par certificat : (mode unique et routé uniquement) Lorsque vous activez l'authentification ASDM (HTTPS), vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Si le nom d'utilisateur et le mot de passe sont différents pour l'authentification par certificat, vous êtes invité à les saisir également. Vous pouvez choisir de préremplir le nom d'utilisateur dérivé de votre certificat.

À propos de l'authentification série

Consultez le comportement suivant pour l'accès au port de console série avec et sans authentification :

- Aucune authentification : si vous n'activez aucune authentification pour l'accès en série, vous ne saisissez pas de nom d'utilisateur ni de mot de passe. Vous accédez au mode EXEC de l'utilisateur.

- Authentification : si vous activez l'authentification pour l'accès en série, vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'activation de l'authentification

Pour passer en mode d'exécution privilégié après la connexion, saisissez la commande **enable**. Le fonctionnement de cette commande dépend de si vous activez ou non l'authentification.

- Aucune authentification : si vous ne configurez pas l'authentification, saisissez le mot de passe d'activation du système lorsque vous saisissez la commande **enable** (défini par la commande **enable password**), qui est vide par défaut. La première fois que vous saisissez la commande **enable**, vous devez modifier le mot de passe. Cependant, si vous n'utilisez pas l'activation de l'authentification, après avoir saisi la commande **enable**, vous n'êtes plus connecté en tant qu'utilisateur particulier, ce qui peut affecter les fonctionnalités basées sur l'utilisateur telles que l'autorisation de commande. Pour conserver votre nom d'utilisateur, utilisez l'activation de l'authentification.
- Authentification : si vous configurez l'activation de l'authentification, l'ASA vous invite à entrer votre nom d'utilisateur et mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Cette fonctionnalité est particulièrement utile lorsque vous effectuez une autorisation de commande, dans laquelle les noms d'utilisateur sont importants pour déterminer les commandes qu'un utilisateur peut saisir.

Pour activer l'authentification à l'aide de la base de données locale, vous pouvez utiliser la commande **login** au lieu de la commande **enable**. La commande **login** conserve le nom d'utilisateur, mais ne nécessite aucune configuration pour activer l'authentification.

⚠

Mise en garde Si vous ajoutez à la base de données locale des utilisateurs qui peuvent accéder à l'interface de ligne de commande et que vous ne souhaitez pas entrer en mode d'exécution privilégié, vous devez configurer l'autorisation de commande. Sans autorisation de commande, les utilisateurs peuvent accéder au mode d'exécution privilégié (et à toutes les commandes) au niveau de l'interface de ligne de commande en utilisant leur propre mot de passe si leur niveau de privilège est de 2 ou plus (2 est la valeur par défaut). Vous pouvez également décourager l'utilisation de la commande login en utilisant un serveur AAA pour l'authentification au lieu de la base de données locale, ou vous pouvez définir tous les utilisateurs locaux au niveau 1 afin de pouvoir contrôler qui peut utiliser le mot de passe d'activation du système pour accéder au mode d'exécution privilégié.

Sessions du système d'exploitation hôte vers l'ASA

Certaines plateformes prennent en charge l'exécution de l'ASA en tant qu'application distincte : par exemple l'ASA sur le Firepower 4100/9300. Pour les sessions du système d'exploitation hôte à l'ASA, vous pouvez configurer l'authentification série et Telnet, selon le type de connexion. Par exemple, la commande **connect asa** dans FXOS sur le Firepower 2100 en mode plateforme utilise un port série.

En mode de contexte multiple, vous ne pouvez pas configurer de commandes AAA dans la configuration système. Cependant, si vous configurez l'authentification Telnet ou série dans le contexte d'administration, l'authentification s'applique également à ces sessions. Le serveur AAA du contexte d'administration ou la base de données locale des utilisateurs est utilisé dans cette instance.

Configurer l'authentification pour l'interface de ligne de commandeet ASDM Access

Avant de commencer

- Configurez l'accès Telnet, SSH ou HTTP.
- Pour l'authentification extérieure, configurez un groupe de serveurs AAA. Pour l'authentification locale, ajoutez des utilisateurs à la base de données locale.
- L'authentification de gestion HTTP ne prend pas en charge le protocole SDI pour un groupe de serveurs AAA.
- Cette fonctionnalité n'affecte pas l'authentification par clé publique SSH pour les noms d'utilisateur locaux avec la commande **ssh authentication**. L'ASA utilise implicitement la base de données locale pour l'authentification par clé publique. Cette fonctionnalité n'affecte que les noms d'utilisateur avec mots de passe. Si vous souhaitez autoriser l'authentification par clé publique ou l'utilisation du mot de passe par un utilisateur local, vous devez configurer explicitement l'authentification locale à l'aide de cette procédure pour autoriser l'accès par mot de passe.

Procédure

Authentifiez les utilisateurs pour l'accès de la gestion.

aaa authentication {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

Exemple :

```
ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL
ciscoasa(config)# aaa authentication http console radius_1 LOCAL
ciscoasa(config)# aaa authentication serial console LOCAL
```

Le mot clé **telnet** contrôle l'accès Telnet. Le mot clé **ssh** contrôle l'accès SSH (mot de passe uniquement; l'authentification par clé publique utilise implicitement la base de données locale). Le mot clé **http** contrôle l'accès ASDM. Le mot clé **serial** contrôle l'accès au port de la console. Pour Firepower 2100 en mode plateforme, ce mot clé affecte la console virtuelle accessible à partir de FXOS à l'aide de la commande **connect asa**.

Si vous utilisez un groupe de serveurs AAA pour l'authentification, vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Spécifiez le nom du groupe de serveurs suivi de **LOCAL** (qui est sensible à la casse). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée. Vous pouvez également utiliser la base de données locale comme méthode d'authentification principale (sans système de secours) en saisissant **LOCAL** uniquement.

Configurer l'activation de l'authentification (mode d'exécution privilégié)

Vous pouvez authentifier les utilisateurs lorsqu'ils saisissent la commande **enable**.

Avant de commencer

Consultez À propos de l'activation de l'authentification, à la page 1298.

Procédure

Choisissez l'une des options suivantes pour l'authentification des utilisateurs :

- Pour authentifier les utilisateurs auprès d'un serveur AAA ou de la base de données locale, saisissez la commande suivante :

  aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]}

  Exemple :

  ```
  ciscoasa(config)# aaa authentication enable console LOCAL
  ```

  Un nom d'utilisateur et un mot de passe seront demandés à l'utilisateur.

  Si vous utilisez un groupe de serveurs AAA pour l'authentification, vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Spécifiez le nom du groupe de serveurs suivi de **LOCAL** (qui est sensible à la casse). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée.

  Vous pouvez également utiliser la base de données locale comme méthode d'authentification principale (sans système de secours) en saisissant **LOCAL** uniquement.

- Pour vous connecter en tant qu'utilisateur à partir de la base de données locale, saisissez la commande suivante :

  login

  Exemple :

  ```
  ciscoasa# login
  ```

  L'ASA vous demande votre nom d'utilisateur et votre mot de passe. Après avoir saisi votre mot de passe, l'ASA vous place au niveau de privilège spécifié par la base de données locale.

  Les utilisateurs peuvent se connecter avec leur nom d'utilisateur et mot de passe pour accéder au mode d'exécution privilégié. Vous n'avez donc pas à fournir le mot de passe d'activation du système à tout le monde. Pour permettre aux utilisateurs d'accéder au mode d'exécution privilégié (et à toutes les commandes) lorsqu'ils se connectent, définissez le niveau de privilège de l'utilisateur de 2 (par défaut) à 15. Si vous configurez l'autorisation de commande locale, l'utilisateur ne peut entrer que les commandes attribuées à ce niveau de privilège ou à un niveau inférieur.

Configurer l'authentification par certificat ASDM

Vous pouvez exiger l'authentification par certificat, avec ou sans authentification AAA. L'ASA valide le certificat par rapport au point de confiance PKI.

Avant de commencer

Cette fonctionnalité est prise en charge uniquement en mode routé simple.

Procédure

Étape 1 Activez l'authentification par certificat :

http authentication-certificate *interface_name*[**match** *certificate_map_name*]

Exemple :

```
ciscoasa(config)# crypto ca certificate map map1 10
ciscoasa(config-ca-cert-map)# subject-name emailAddress www.example.com
ciscoasa(config)# http authentication-certificate outside match map1
```

Vous configurez l'authentification par certificat pour chaque interface, de sorte que les connexions sur une interface de confiance/interne n'ont pas à fournir de certificat. Vous pouvez utiliser la commande plusieurs fois pour activer l'authentification par certificat sur plusieurs interfaces.

Pour exiger que le certificat corresponde à une carte de certificat, spécifiez le mot clé **match** et le nom de la carte. Configurez la carte à l'aide de la commande **crypto ca certificate map**.

Étape 2 (Facultatif) Définissez l'attribut utilisé par ASDM pour dériver le nom d'utilisateur à partir du certificat :

http username-from-certificate{*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**} [**pre-fill-username**]

Exemple :

```
ciscoasa(config)# http username-from-certificate CN pre-fill-username
```

Par défaut, ASDM utilise les attributs CN OU.

- L'argument *primary-attr* spécifie l'attribut à utiliser pour dériver le nom d'utilisateur. L'argument *secondary-attr* spécifie un attribut supplémentaire à utiliser avec l'attribut principal pour dériver le nom d'utilisateur. Vous pouvez utiliser les attributs suivants :
  - C : Pays
  - CN : nom commun
  - DNQ : qualificateur de nom distinctif
  - emailAddress : adresse courriel
  - GENQ : qualificatif générationnel
  - GN : prénom
  - I : initiales
  - L : localité
  - N : nom
  - O : organisation
  - OU : unité organisationnelle

- SER : numéro de série
- SN : nom de famille
- SP : État/province
- T : titre
- UID : identifiant de l'utilisateur
- UPN : nom principal de l'utilisateur

- Le mot clé **use-entire-name** utilise le nom complet du DN.
- Le mot clé **use-script** utilise un script Lua généré par ASDM.
- Le mot clé **pre-fill-username** préremplit le nom d'utilisateur lorsque l'authentification est demandée. Si le nom d'utilisateur est différent de celui que vous avez initialement saisi, une nouvelle boîte de dialogue s'affiche avec le nom d'utilisateur prérempli. Vous pouvez ensuite saisir le mot de passe pour l'authentification.

Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion

L'ASA vous permet de distinguer les utilisateurs administratifs et d'accès à distance lorsqu'ils s'authentifient. La différence des rôles d'utilisateur peut empêcher les utilisateurs du VPN d'accès à distance et de l'accès réseau d'établir une connexion administrative à l'ASA.

Avant de commencer

Utilisateurs RADIUS ou LDAP (mappés)

Lorsque les utilisateurs sont authentifiés par LDAP, les attributs LDAP natifs et leurs valeurs peuvent être mappés aux attributs ASA pour fournir des fonctionnalités d'autorisation spécifiques. Configurez Cisco VSA CVPN3000-Privilege-Level avec une valeur comprise entre 0 et 15, puis mappez les attributs LDAP à Cisco VAS CVPN3000-Privilege-Level à l'aide de la commande **ldap map-attributes**.

L'attribut **service-type** IETF RADIUS, lorsqu'il est envoyé dans un message d'acceptation de l'accès à la suite d'une demande d'authentification et d'autorisation RADIUS, est utilisé pour désigner le type de service accordé à l'utilisateur authentifié.

L'attribut **privilege-level** RADIUS Cisco VSA (ID de fournisseur 3076, sous-ID 220), lorsqu'il est envoyé dans un message d'acceptation de l'accès, est utilisé pour désigner le niveau de privilège de l'utilisateur.

Utilisateurs TACACS+

L'autorisation est demandée par « service=shell », et le serveur répond par PASS (réussite) ou FAIL (échec).

Utilisateurs locaux

Définissez la commande **service-type** pour un nom d'utilisateur donné. Par défaut, le type de service est admin, ce qui permet un accès complet à tous les services spécifiés par la commande **aaa authentication console**.

Attributs d'autorisation de gestion

Consultez le tableau suivant pour connaître les types de serveurs AAA et les valeurs valides pour l'autorisation de gestion. L'ASA utilise ces valeurs pour déterminer le niveau d'accès de gestion.

Niveau de gestion	Attributs RADIUS/LDAP (mappés)	Attributs TACACS+	Attributs de la base de données locale
Accès complet : permet un accès complet à tous les services spécifiés par les commandes **aaa authentication console**	Type de service 6 (Administrateur), niveau de privilège 1	PASS (réussite), privilège de niveau 1	admin
Accès partiel : permet l'accès à l'interface de ligne de commande ou à ASDM lorsque vous configurez les commandes **aaa authentication console** . Cependant, si vous configurez l'authentification **enable** avec la commande **aaa authentication enable console** option, l'utilisateur de l'interface de ligne de commande ne peut pas accéder au mode d'exécution privilégié à l'aide de la commande **enable**.	Type de service 7 (invite NAS), niveau de privilège 2 et supérieur Les types de service Framed (2) et Login (1) sont traités de la même manière.	PASS (réussite), niveau de privilège 2 et supérieur	nas-prompt
Aucun accès : refuse l'accès de gestion. L'utilisateur ne peut pas utiliser les services spécifiés par les commandes **aaa authentication console** (à l'exception du mot clé **serial** option; l'accès en série est autorisé). Les utilisateurs d'accès à distance (IPsec et SSL) peuvent toujours s'authentifier et mettre fin à leurs sessions d'accès à distance. Tous les autres types de services (voix, FAX, etc.) sont traités de la même manière.	Type de service 5 (sortant)	ÉCHEC	remote-access

Directives supplémentaires

- L'accès à la console de série n'est pas inclus dans l'autorisation de gestion.
- Vous devez également configurer l'authentification AAA pour l'accès de gestion afin d'utiliser cette fonctionnalité. Consultez Configurer l'authentification pour l'interface de ligne de commandeet ASDM Access, à la page 1299.
- Si vous utilisez l'authentification extérieure, vous devez préconfigurer un groupe de serveurs AAA avant d'activer cette fonctionnalité.
- L'autorisation HTTP est prise en charge uniquement en mode routé simple.

Procédure

Étape 1 Activez l'autorisation de gestion pour Telnet et SSH :

aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

Le mot clé **auto-enable** permet aux administrateurs disposant de privilèges d'autorisation suffisants de passer automatiquement en mode d'exécution privilégié lorsqu'ils se connectent.

Exemple :

```
ciscoasa(config)# aaa authentication ssh console RADIUS
ciscoasa(config)# aaa authorization exec authentication-server auto-enable
```

Étape 2 Activez l'autorisation de gestion pour HTTPS (ASDM) :

aaa authorization http console {**authentication-server** | **LOCAL**}

Exemple :

```
ciscoasa(config)# aaa authentication http console RADIUS
ciscoasa(config)# aaa authorization http console authentication-server
```

Étape 3

Exemples

L'exemple suivant montre comment définir une carte d'attributs LDAP. Dans cet exemple, la stratégie de sécurité précise que les utilisateurs authentifiés par LDAP mappent les champs d'enregistrement d'utilisateur ou le titre des paramètres et la société au type de service et au niveau de privilège IETF-RADIUS, respectivement.

```
ciscoasa(config)# ldap attribute-map admin-control
ciscoasa(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
ciscoasa(config-ldap-attribute-map)# map-name company
```

L'exemple suivant applique une carte d'attributs LDAP à un serveur LDAP AAA :

```
ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
ciscoasa(config-aaa-server-host)# ldap attribute-map admin-control
```

Configurer l'autorisation de commande

Si vous souhaitez contrôler l'accès aux commandes, l'ASA vous permet de configurer l'autorisation de commande, dans laquelle vous pouvez déterminer quelles commandes sont disponibles pour un utilisateur. Par défaut, lorsque vous vous connectez, vous pouvez accéder au mode EXEC de l'utilisateur, qui n'offre que des commandes minimales. Lorsque vous saisissez la commande **enable** (ou la commande **login** lorsque vous utilisez la base de données locale), vous pouvez accéder au mode d'exécution privilégié et aux commandes avancées, y compris les commandes de configuration.

Vous pouvez utiliser l'une des deux méthodes d'autorisation de commande suivantes :

- Niveaux de privilèges locaux
- Niveaux de privilèges du serveur TACACS+

À propos de l'autorisation de commande

Vous pouvez activer l'autorisation de commande pour que seuls les utilisateurs autorisés puissent saisir des commandes.

Méthodes d'autorisation de commande prises en charge

Vous pouvez utiliser l'une des deux méthodes d'autorisation de commande suivantes :

- Niveaux de privilèges locaux : configurez les niveaux de privilège de commande sur l'ASA. Lorsqu'un utilisateur local, RADIUS ou LDAP (si vous mappez des attributs LDAP aux attributs RADIUS) s'authentifie pour l'accès à l'interface de ligne de commande, l'ASA place cet utilisateur au niveau de privilège défini par la base de données locale, RADIUS ou le serveur LDAP. L'utilisateur peut accéder aux commandes au niveau de privilège attribué et en dessous. Notez que tous les utilisateurs accèdent au mode EXEC lorsqu'ils se connectent pour la première fois (commandes au niveau 0 ou 1). L'utilisateur doit s'authentifier de nouveau avec la commande **enable** pour accéder au mode d'exécution privilégié (commandes de niveau 2 ou supérieur), ou il peut se connecter avec la commande **login** (base de données locale uniquement).



Remarque Vous pouvez utiliser l'autorisation de commande locale sans aucun utilisateur dans la base de données locale et sans interface de ligne de commande ni authentification **enable**. Au lieu de cela, lorsque vous saisissez la commande **enable**, vous saisissez le mot de passe d'activation du système et l'ASA vous place au niveau 15. Vous pouvez ensuite créer des mots de passe d'activation pour chaque niveau, de sorte que lorsque vous entrez **enable** *n* (2 à 15), l'ASA vous place au niveau *n*. Ces niveaux ne sont pas utilisés, sauf si vous activez l'autorisation de commande locale.

- Niveaux de privilège du serveur TACACS+ : sur le serveur TACACS+, configurez les commandes qu'un utilisateur ou un groupe peut utiliser après s'être authentifié pour l'accès à l'interface de ligne de commande. Chaque commande qu'un utilisateur saisit au niveau de l'interface de ligne de commande est validée auprès du serveur TACACS+.

Contextes de sécurité et autorisation de commande

Les paramètres AAA sont distincts par contexte et ne sont pas partagés entre les contextes.

Lors de la configuration de l'autorisation de commande, vous devez configurer chaque contexte de sécurité séparément. Cette configuration vous offre la possibilité d'appliquer différentes autorisations de commande pour différents contextes de sécurité.

Lorsqu'ils passent d'un contexte de sécurité à l'autre, les administrateurs doivent savoir que les commandes autorisées pour le nom d'utilisateur spécifié lors de la connexion peuvent être différentes dans la nouvelle session de contexte ou que l'autorisation de commande peut ne pas être configurée du tout dans le nouveau contexte. Ne pas comprendre que les autorisations de commande peuvent différer d'un contexte de sécurité à l'autre peut dérouter un administrateur.



Remarque L'espace d'exécution du système ne prend pas en charge les commandes AAA; par conséquent, l'autorisation de commande n'est pas disponible dans l'espace d'exécution du système.

Niveaux de privilège de commande

Par défaut, les commandes suivantes sont affectées au niveau de privilège 0. Toutes les autres commandes sont affectées au niveau de privilège 15.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

Si vous déplacez des commandes de mode de configuration à un niveau inférieur à 15, veillez également à déplacer la commande **configure** à ce niveau, sinon l'utilisateur ne pourra pas entrer en mode de configuration.

Configurer l'autorisation de commande locale

L'autorisation de commande locale vous permet d'affecter des commandes à l'un des 16 niveaux de privilège (0 à 15). Par défaut, chaque commande est affectée au niveau de privilège 0 ou 15. Vous pouvez définir chaque utilisateur comme étant à un niveau de privilège spécifique, et chaque utilisateur peut saisir n'importe quelle commande au niveau de privilège attribué ou en dessous. L'ASA prend en charge les niveaux de privilège d'utilisateur définis dans la base de données locale, un serveur RADIUS ou un serveur LDAP (si vous mappez des attributs LDAP aux attributs RADIUS).

Procédure

Étape 1 Attribuez une commande à un niveau de privilège.

privilege [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command*

Exemple :

```
ciscoasa(config)# privilege show level 5 command filter
```

Répétez cette commande pour chaque commande que vous souhaitez réaffecter.

Les options de cette commande sont les suivantes :

- **show** | **clear** | **cmd** : ces mots clés facultatifs vous permettent de définir les privilèges uniquement pour la forme show, clear ou configure de la commande. La forme configure de la commande est généralement la forme qui entraîne une modification de configuration, soit sous forme de commande non modifiée (sans le préfixe **show** ou **clear**), soit sous la forme **no**. Si vous n'utilisez pas l'un de ces mots clés, toutes les formes de commande sont affectées.
- **level** *level* : un niveau compris entre 0 et 15.
- **mode** {**enable** | **configure**} : si une commande peut être saisie en mode d'exécution privilégié ainsi qu'en mode de configuration et que la commande effectue des actions différentes dans chaque mode, vous pouvez définir le niveau de privilège pour ces modes séparément :
  - **enable** : spécifie le mode EXEC de l'utilisateur et le mode d'exécution privilégié.
  - **configure** : spécifie le mode de configuration, accessible à l'aide de la commande **configure terminal**.
- **command** *command* : la commande que vous configurez. Vous pouvez uniquement configurer le niveau de privilège de la commande *principale*. Par exemple, vous pouvez configurer le niveau de toutes les commandes **aaa**, mais pas le niveau des commandes **aaa authentication** et **aaa authorization** séparément.

Étape 2 (Facultatif) Activez les utilisateurs AAA pour l'autorisation de commande. Sans cette commande, l'ASA ne prend en charge que les niveaux de privilège des utilisateurs de base de données locaux et définit par défaut tous les autres types d'utilisateurs au niveau 15.

aaa authorization exec authentication-server [auto-enable]

Exemple :

```
ciscoasa(config)# aaa authorization exec authentication-server
```

Cette commande active également l'autorisation de gestion. Consultez Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion, à la page 1302.

Étape 3 Activez l'utilisation des niveaux de privilège de commande locaux :

aaa authorization command LOCAL

Exemple :

```
ciscoasa(config)# aaa authorization command LOCAL
```

Lorsque vous définissez des niveaux de privilège de commande, l'autorisation de commande n'a pas lieu, sauf si vous configurez l'autorisation de commande avec cette commande.

Exemples

La commande **filter** a les formes suivantes :

- **filter** (représenté par l'option **configure**)
- **show running-config filter**

- **clear configure filter**

Vous pouvez définir le niveau de privilège séparément pour chaque formulaire ou définir le même niveau de privilège pour tous les formulaires en omettant cette option. L'exemple suivant montre comment définir chaque formulaire séparément :

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

Sinon, l'exemple suivant montre comment définir toutes les commandes de filtre au même niveau :

```
ciscoasa(config)# privilege level 5 command filter
```

La commande **show privilege** sépare les formulaires dans l'affichage.

L'exemple suivant montre l'utilisation du mot clé **mode**. La commande **enable** doit être saisie à partir du mode EXEC de l'utilisateur, tandis que la commande **enable password**, qui est accessible en mode de configuration, requiert le niveau de privilège le plus élevé :

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

L'exemple suivant montre une commande supplémentaire, la commande **configure**, qui utilise le mot clé **mode** :

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
ciscoasa(config)# privilege clear level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```

Remarque Cette dernière ligne est pour la commande **configure terminal**.

Configurer les commandes sur le serveur TACACS+

Vous pouvez configurer des commandes sur un serveur TACACS+ Cisco Secure Access Control Server (ACS) en tant que composant de profil partagé, pour un groupe ou pour des utilisateurs individuels. Pour les serveurs TACACS+ tiers, consultez la documentation de votre serveur pour en savoir plus sur la prise en charge des autorisations de commandes.

Consultez les lignes directrices suivantes pour la configuration des commandes dans Cisco Secure ACS version 3.1; la plupart de ces lignes directrices s'appliquent également aux serveurs tiers :

- L'ASA envoie les commandes à autoriser en tant que commandes shell; veuillez donc configurer les commandes sur le serveur TACACS+ en tant que commandes shell.

Remarque Cisco Secure ACS peut inclure un type de commande appelé « pix-shell ». N'utilisez pas ce type pour l'autorisation de commande ASA.

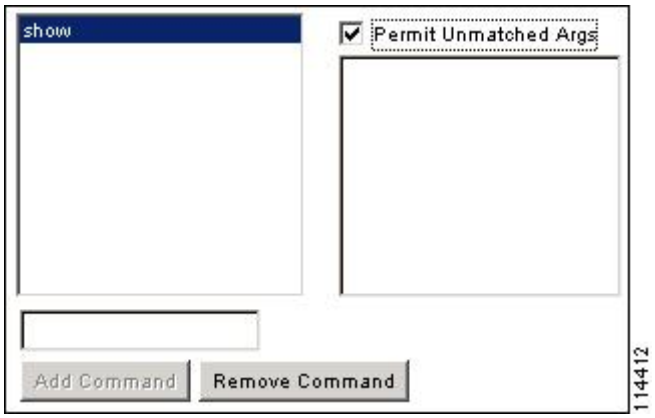
- Le premier mot de la commande est considéré comme la commande principale. Tous les mots supplémentaires sont considérés comme des arguments, qui doivent être précédés de **permit** ou **deny**.

  Par exemple, pour autoriser la commande **show running-configuration aaa-server**, ajoutez **show running-configuration** dans le champ de la commande et saisissez **permit aaa-server** dans le champ des arguments.

- Vous pouvez autoriser tous les arguments d'une commande que vous ne refusez pas explicitement en cochant la case **Permit Unmatched Args** (Autoriser les arguments sans correspondance).

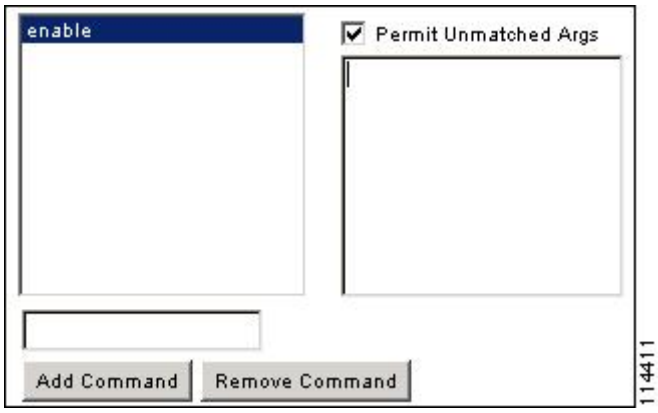
  Par exemple, vous pouvez configurer uniquement la commande **show**. Toutes les commandes **show** sont autorisées. Nous vous conseillons d'utiliser cette méthode pour que vous n'ayez pas à anticiper chaque variante d'une commande, y compris les abréviations et un point d'interrogation, qui indique l'utilisation de l'interface de ligne de commande (voir la figure suivante).

Illustration 75 : Autoriser toutes les commandes associées



- Pour les commandes composées d'un seul mot, vous *devez* autoriser des arguments sans correspondance, même s'il n'y a aucun argument pour la commande, par exemple **enable** ou **help** (voir la figure suivante).

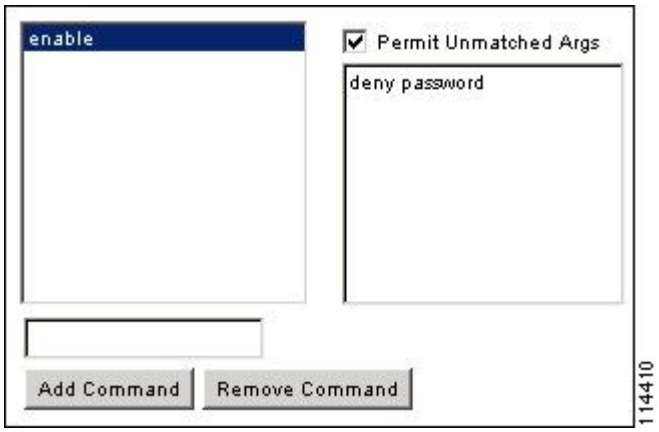
Illustration 76 : Autorisation des commandes à un seul mot



- Pour interdire certains arguments, entrez les arguments précédés de **deny**.

  Par exemple, pour autoriser **enable**, mais pas **enable password**, saisissez **enable** dans le champ des commandes et **deny password** dans le champ des arguments. Assurez-vous de cocher la case **Permit Unmatched Args** (Autoriser les arguments sans correspondance) pour que **enable** soit toujours autorisé (voir la figure suivante).

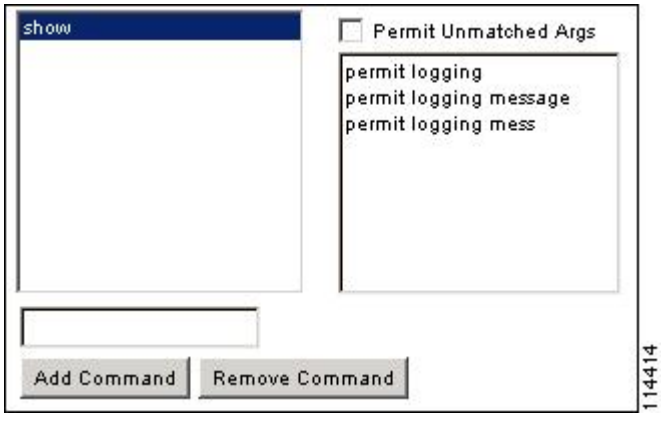
  Illustration 77 : Interdire les arguments



- Lorsque vous abrégez une commande dans la ligne de commande, l'ASA développe le préfixe et la commande principale en texte intégral, mais envoie des arguments supplémentaires au serveur TACACS+ au fur et à mesure que vous les saisissez.

  Par exemple, si vous saisissez **sh log**, l'ASA envoie la commande complète au serveur TACACS+, **show logging**. Cependant, si vous saisissez **sh log mess**, l'ASA envoie **show logging mess** au serveur TACACS+, et non la commande étendue **show logging message**. Vous pouvez configurer plusieurs orthographes du même argument afin d'anticiper les abréviations (voir la figure suivante).

  Illustration 78 : Spécifier les abréviations



- Nous vous conseillons d'autoriser les commandes de base suivantes pour tous les utilisateurs :
  - **show checksum**
  - **show curpriv**
  - **enable**

- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

Configurer l'autorisation de commande TACACS+

Si vous activez l'autorisation de commande TACACS+ et qu'un utilisateur saisit une commande au niveau de l'interface de ligne de commande, l'ASA envoie la commande et le nom d'utilisateur au serveur TACACS+ pour déterminer si la commande est autorisée.

Avant d'activer l'autorisation de commande TACACS+, assurez-vous d'être connecté à l'ASA en tant qu'utilisateur défini sur le serveur TACACS+ et de disposer de l'autorisation de commande nécessaire pour continuer à configurer l'ASA. Par exemple, vous devez vous connecter en tant qu'utilisateur admin avec toutes les commandes autorisées. Sinon, vous pourriez vous retrouver involontairement bloqué.

N'enregistrez pas votre configuration avant d'être sûr qu'elle fonctionne comme vous le souhaitez. Si vous êtes bloqué par erreur, vous pouvez généralement récupérer l'accès en redémarrant l'ASA.

Assurez-vous que votre système TACACS+ est complètement stable et fiable. Le niveau de fiabilité nécessaire exige généralement que vous ayez un système de serveurs TACACS+ entièrement redondant et une connectivité entièrement redondante à l'ASA. Par exemple, dans votre ensemble de serveurs TACACS+, incluez un serveur connecté à l'interface 1 et un autre à l'interface 2. Vous pouvez également configurer l'autorisation de commande locale comme méthode de secours si le serveur TACACS+ n'est pas disponible.

Pour configurer l'autorisation de commande à l'aide d'un serveur TACACS+, procédez comme suit :

Procédure

Entrez la commande suivante :

aaa authorization command *tacacs+_server_group* [**LOCAL**]

Exemple :

```
ciscoasa(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

Vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur TACACS+ n'est pas disponible. Pour activer le basculement, précisez le nom du groupe de serveurs suivi de **LOCAL** (**LOCAL** est sensible à la casse). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur TACACS+, car l'invite ASA n'indique

pas quelle méthode est utilisée. Assurez-vous de configurer les utilisateurs dans la base de données locale et les niveaux de privilège de commande.

Configurer une politique de mot de passe pour les utilisateurs de base de données locale

Lorsque vous configurez l'authentification pour l'accès à l'interface de ligne de commande ou à ASDM à l'aide de la base de données locale, vous pouvez configurer une politique de mot de passe qui oblige un utilisateur à changer de mot de passe après une durée spécifiée et qui exige également des normes de mot de passe telles qu'une longueur minimum et le nombre minimum de modifications de caractères.

La politique de mot de passe s'applique uniquement aux utilisateurs administratifs qui utilisent la base de données locale et non aux autres types de trafic qui peuvent utiliser la base de données locale, comme le VPN ou l'AAA pour l'accès au réseau, et non aux utilisateurs authentifiés par un serveur AAA.

Après avoir configuré la politique de mot de passe, lorsque vous modifiez un mot de passe (le vôtre ou celui d'un autre utilisateur), la politique de mot de passe s'applique au nouveau mot de passe. Tous les mots de passe existants sont conservés. La nouvelle politique s'applique à la modification du mot de passe avec la commande **username** et la commande **change-password**.

Avant de commencer

- Configurez l'authentification AAA pour l'accès de l'interface de ligne de commande ou ASDM à l'aide de la base de données locale.
- Spécifiez les noms d'utilisateurs dans la base de données locale.

Procédure

Étape 1 (Facultatif) Définissez l'intervalle en jours après lequel les mots de passe expirent pour les utilisateurs distants.

password-policy lifetime *days*

Exemple :

```
ciscoasa(config)# password-policy lifetime 180
```

Remarque
Les utilisateurs au niveau du port de console ne sont jamais verrouillés en raison de l'expiration du mot de passe.

Les valeurs valides sont comprises entre 0 et 65536 jours. La valeur par défaut est 0 jour, une valeur indiquant que les mots de passe n'expireront jamais.

Sept jours avant l'expiration du mot de passe, un message d'avertissement s'affiche. À l'expiration du mot de passe, l'accès au système est refusé aux utilisateurs distants. Pour y accéder après l'expiration, effectuez l'une des opérations suivantes :

- Demandez à un autre administrateur de modifier votre mot de passe à l'aide de la commande **username**.

- Connectez-vous au port de console physique pour modifier votre mot de passe.

Étape 2 (Facultatif) Définissez le nombre minimum de caractères que vous devez modifier entre l'ancien et le nouveau mot de passe.

password-policy minimum-changes *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-changes 2
```

Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0.

La correspondance des caractères est indépendante de la position, ce qui signifie que les caractères du nouveau mot de passe ne sont considérés comme modifiés que s'ils n'apparaissent nulle part dans le mot de passe actuel.

Étape 3 (Facultatif) Définissez la longueur minimum des mots de passe.

password-policy minimum-length *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-length 8
```

Les valeurs valides sont comprises entre 3 et 64 caractères. Nous conseillons un mot de passe d'une longueur minimum de 8 caractères.

Étape 4 (Facultatif) Définissez le nombre minimum de caractères majuscules que les mots de passe doivent contenir.

password-policy minimum-uppercase *value*

Exemple :

```
ciscoasa(config)# password-policy  minimum-uppercase 3
```

Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0, ce qui signifie qu'il n'y a pas de minimum.

Étape 5 (Facultatif) Définissez le nombre minimum de caractères minuscules que les mots de passe doivent contenir.

password-policy minimum-lowercase *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0, ce qui signifie qu'il n'y a pas de minimum.

Étape 6 (Facultatif) Définissez le nombre minimum de caractères numériques que les mots de passe doivent contenir.

password-policy minimum-numeric *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-numeric 1
```

Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0, ce qui signifie qu'il n'y a pas de minimum.

Étape 7 (Facultatif) Définissez le nombre minimum de caractères spéciaux que les mots de passe doivent contenir.

password-policy minimum-special *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-special 2
```

Les valeurs valides sont comprises entre 0 et 64 caractères. Les caractères spéciaux sont les suivants : !, @, #, $, %, ^, &, *, « (» et «) ». La valeur par défaut est 0, ce qui signifie qu'il n'y a pas de minimum.

Étape 8 Interdire la réutilisation d'un mot de passe :

password-policy reuse-interval *value*

Exemple :

```
ciscoasa(config)# password-policy reuse-interval 5
```

Vous pouvez interdire la réutilisation d'un mot de passe correspondant aux mots de passe utilisés précédemment, entre 2 et 7 mots de passe précédents. Les mots de passe précédents sont stockés dans la configuration sous chaque nom d'utilisateur sous forme chiffrée à l'aide de la commande **password-history**; cette commande n'est pas configurable par l'utilisateur.

Étape 9 Interdire un mot de passe correspondant à un nom d'utilisateur :

password-policy username-check

Étape 10 (Facultatif) Définissez si les utilisateurs doivent modifier leur mot de passe à l'aide de la commande **change-password**, au lieu de permettre aux utilisateurs de modifier leur mot de passe avec la commande **username**.

password-policy authenticate enable

Exemple :

```
ciscoasa(config)# password-policy authenticate enable
```

Le paramètre par défaut est désactivé : un utilisateur peut utiliser l'une ou l'autre des méthodes pour modifier son mot de passe.

Si vous activez cette fonctionnalité et essayez de modifier votre mot de passe à l'aide de la commande **username**, le message d'erreur suivant s'affiche :

```
ERROR: Changing your own password is prohibited
```

Vous ne pouvez pas non plus supprimer votre propre compte avec la commande **clear configure username**. Si vous essayez, le message d'erreur suivant s'affiche :

```
ERROR: You cannot delete all usernames because you are not allowed to delete yourself
```

Changer votre mot de passe

Si vous configurez une durée de validité du mot de passe dans la politique de mot de passe, vous devez changer votre mot de passe lorsque l'ancien mot de passe expire. Cette méthode de modification du mot de passe est requise si vous activez l'authentification par politique de mot de passe. Si l'authentification par politique de mot de passe n'est pas activée, vous pouvez utiliser cette méthode ou vous pouvez modifier directement votre compte d'utilisateur.

Pour modifier votre mot de passe d'utilisateur, procédez comme suit :

Procédure

Entrez la commande suivante :

change-password [**old-password** *old_password* [**new-password** *new_password*]]

Exemple :

```
ciscoasa# change-password old-password j0hncr1chton new-password a3rynsun
```

Si vous ne saisissez pas l'ancien et le nouveau mot de passe dans la commande, l'ASA vous invite à les saisir.

Activer et afficher l'historique de connexion

Par défaut, l'historique de connexion est enregistré pendant 90 jours. Vous pouvez désactiver cette fonctionnalité ou modifier la durée, jusqu'à 365 jours.

Avant de commencer

- L'historique de connexion n'est enregistré que par unité; dans les environnements de basculement et de mise en grappe, chaque unité conserve uniquement son propre historique de connexion.
- Les données de l'historique de connexion ne sont pas conservées pendant les rechargements.
- Cette fonctionnalité s'applique aux noms d'utilisateur dans la base de données locale ou à partir d'un serveur AAA lorsque vous activez l'authentification AAA locale pour une ou plusieurs des méthodes de gestion de l'interface de ligne de commande (SSH, Telnet, console série). Les connexions à ASDM ne sont pas enregistrées dans l'historique.

Procédure

Étape 1 Définissez la durée de l'historique de connexion :

aaa authentication login-history duration *days*

Exemple :

```
ciscoasa(config)# aaa authentication login-history duration 365
```

Vous pouvez définir les *jours* entre 1 et 365. La valeur par défaut est 90. Pour désactiver l'historique de connexion, saisissez **no aaa authentication login-history**.

Lorsqu'un utilisateur se connecte, il voit son propre historique de connexion, comme cet exemple SSH :

```
cugel@10.86.194.108's password:
The privilege level for user cugel is 15.  The privilege level at the previous login was
2.
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

Étape 2 Affichez l'historique de connexion :

show aaa login-history [**user** *name*]

Exemple :

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

Configurer la traçabilité de l'accès de gestion

Vous pouvez envoyer des messages de traçabilité au serveur de comptabilité TACACS+ lorsque vous saisissez une commande autre que les commandes **show** au niveau de l'interface de ligne de commande. Vous pouvez configurer la comptabilisation lorsque les utilisateurs se connectent, lorsqu'ils saisissez la commande **enable** ou lorsqu'ils émettent des commandes.

Pour la traçabilité des commandes, vous pouvez uniquement utiliser des serveurs TACACS+.

Pour configurer l'accès de gestion et activer la traçabilité des commandes, procédez comme suit :

Procédure

Étape 1 Entrez la commande suivante :

aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

Exemple :

```
ciscoasa(config)# aaa accounting telnet console group_1
```

Les protocoles de groupe de serveurs valides sont RADIUS et TACACS+.

Étape 2 Activez la traçabilité des commandes. Seuls les serveurs TACACS+ prennent en charge la traçabilité des commandes.

aaa accounting command [**privilege** *level*] *server-tag*

Exemple :

```
ciscoasa(config)# aaa accounting command privilege 15 group_1
```

La paire mot clé-argument **privilege** *level* est le niveau de privilège minimum et l'argument *server-tag* est le nom du groupe de serveurs TACACS+ auquel l'ASA doit envoyer des messages de traçabilité des commandes.

Récupérer d'un verrouillage

Dans certaines circonstances, lorsque vous activez l'autorisation de commande ou l'authentification de l'interface de ligne de commande, vous pouvez être verrouillé hors de l'interface de ligne de commande de l'ASA. Vous pouvez généralement récupérer l'accès en redémarrant l'ASA. Cependant, si vous avez déjà enregistré votre configuration, vous pourriez être verrouillé.

Le tableau suivant répertorie les conditions de verrouillage courantes et la façon dont vous pouvez y remédier.

Tableau 56 : Scénarios de verrouillage de l'authentification de l'interface de ligne de commande et de l'autorisation de commande

Fonctionnalités	Condition de verrouillage	Description	Solution de contournement : mode unique	Solution de contournement : mode multiple
Authentification de l'interface de ligne de commande locale	Aucun utilisateur n'a été configuré dans la base de données locale.	Si vous n'avez aucun utilisateur dans la base de données locale, vous ne pouvez pas vous connecter ni ajouter d'utilisateurs.	Connectez-vous et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et ajouter un utilisateur.

Fonctionnalités	Condition de verrouillage	Description	Solution de contournement : mode unique	Solution de contournement : mode multiple
Autorisation de commande TACACS+ Authentification de l'interface de ligne de commande TACACS+ Authentification de l'interface de ligne de commande RADIUS	Le serveur est en panne ou inaccessible et vous n'avez pas configuré la méthode de secours.	Si le serveur est inaccessible, vous ne pouvez pas vous connecter ni saisir de commandes.	1. Connectez-vous et réinitialisez les mots de passe et les commandes AAA. 2. Configurez la base de données locale comme méthode de secours afin de ne pas être verrouillé lorsque le serveur est en panne.	1. Si le serveur est inaccessible en raison d'une configuration de réseau incorrecte sur l'ASA, connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et reconfigurer vos paramètres réseau. 2. Configurez la base de données locale comme méthode de secours afin de ne pas être verrouillé lorsque le serveur est en panne.
Autorisation de commande TACACS+	Vous êtes connecté en tant qu'utilisateur sans privilèges suffisants ou en tant qu'utilisateur qui n'existe pas.	Vous activez l'autorisation de commande, mais vous constatez ensuite que l'utilisateur ne peut plus saisir de commandes.	Corrigez le compte d'utilisateur du serveur TACACS+. Si vous n'avez pas accès au serveur TACACS+ et que vous devez configurer l'ASA immédiatement, connectez-vous à la partition de maintenance et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et terminer les modifications de configuration. Vous pouvez également désactiver l'autorisation de commande jusqu'à ce que vous corrigiez la configuration TACACS+.
Autorisation de commande locale	Vous êtes connecté en tant qu'utilisateur sans privilèges suffisants.	Vous activez l'autorisation de commande, mais vous constatez ensuite que l'utilisateur ne peut plus saisir de commandes.	Connectez-vous et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et changer le niveau d'utilisateur.

Accès au moniteur

Consultez les commandes suivantes pour surveiller l'accès au périphérique :

- **show running-config all privilege all**

  Cette commande affiche les niveaux de privilège de toutes les commandes.

Pour la commande **show running-config all privilege all**, l'ASA affiche l'affectation actuelle de chaque commande de l'interface de ligne de commande à un niveau de privilège. Voici un exemple de sortie de cette commande :

```
ciscoasa(config)# show running-config all  privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
...
```

- **show running-config privilege level** *level*

  Cette commande affiche les commandes pour un niveau de privilège précis. L'argument level est un nombre entier compris entre 0 et 15.

  L'exemple suivant montre les affectations de commandes pour le niveau de privilège 10 :

```
ciscoasa(config)# show running-config all privilege level 10
privilege show level 10 command aaa
```

- **show running-config privilege command** *command*

  Cette commande affiche le niveau de privilège d'une commande en particulier.

  L'exemple suivant montre les affectations de commandes pour la commande **access-list** :

```
ciscoasa(config)# show running-config all privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

- **show curpriv**

  Cette commande affiche l'utilisateur actuellement connecté.

  Voici un exemple de sortie de la commande **show curpriv** :

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

  Le tableau suivant décrit la sortie de la commande **show curpriv**.

Tableau 57 : Description de la sortie de la commande show curpriv

Champ	Description
Username	Nom d'utilisateur. Si vous êtes connecté en tant qu'utilisateur par défaut, le nom est enable_1 (utilisateur EXEC) ou enable_15 (EXEC privilégié).
Niveau de privilège actuel	Les niveaux vont de 0 à 15. À moins que vous ne configuriez l'autorisation de commande locale et n'affectiez des commandes à des niveaux de privilège intermédiaires, les niveaux 0 et 15 sont les seuls niveaux utilisés.
Modes actuels	Les modes d'accès disponibles sont les suivants : • P_UNPR : mode EXEC de l'utilisateur (niveaux 0 et 1) • P_PRIV : mode d'exécution privilégié (niveaux 2 à 15) • P_CONF : mode de configuration

- **show quota management-session** [**ssh** | **telnet** | **http** | **username** *user*]

  Cette commande affiche les sessions actuelles en cours d'utilisation.

  Voici un exemple de sortie de la commande **show quota management-session** :

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                  Username
1                              SSH                      cisco
2                              TELNET                   cisco
1                              SSH                      cisco1
```

- **show aaa login-history** [**user** *name*]

  Cette commande affiche l'historique de connexion par utilisateur.

  Voici un exemple de sortie de la commande **show aaa login-history**.

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

Historique de l'accès de gestion

Tableau 58 : Historique de l'accès de gestion

Nom de la caractéristique	Versions de plateforme	Description
Pile CiscoSSH maintenant par défaut	9.19(1)	La pile Cisco SSH est maintenant utilisée par défaut. Commandes nouvelles ou modifiées : **ssh stack ciscossh**
Prise en charge de l'interface de boucle avec retour pour SSH et Telnet	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour les fonctionnalités suivantes : • SSH • Telnet Commandes nouvelles/modifiées : **interface loopback**, **ssh**, **telnet**
Pile CiscoSSH	9.17(1)	L'ASA utilise une pile SSH propriétaire pour les connexions SSH. Vous pouvez maintenant choisir d'utiliser à la place la pile CiscoSSH, qui est basée sur OpenSSH. La pile par défaut continue d'être la pile ASA. Cisco SSH prend en charge : • Conformité FIPS • Mises à jour régulières, y compris les mises à jour de Cisco et de la communauté de code source libre. Notez que la pile CiscoSSH ne prend pas en charge : • SSH vers une interface différente sur VPN (accès de gestion) • Paire de clés EdDSA • Paire de clés RSA en mode FIPS Si vous avez besoin de ces fonctionnalités, vous devez continuer à utiliser la pile SSH ASA. Il y a une petite modification de la fonctionnalité SCP avec la pile CiscoSSH : pour utiliser la commande **copy** de l'ASA pour copier un fichier vers ou à partir d'un serveur SCP, vous devez activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP à l'aide de la commande **ssh**. Commandes nouvelles ou modifiées : **ssh stack ciscossh**

Nom de la caractéristique	Versions de plateforme	Description
Modifications du verrouillage de l'utilisateur local	9.17(1)	L'ASA peut verrouiller les utilisateurs locaux après un nombre configurable de tentatives de connexion échouées. Cette fonctionnalité ne s'applique pas aux utilisateurs ayant le niveau de privilège 15. De plus, un utilisateur serait verrouillé indéfiniment jusqu'à ce qu'un administrateur déverrouille son compte. Désormais, les utilisateurs seront déverrouillés après 10 minutes, à moins qu'un administrateur n'utilise la commande **clear aaa local user lockout** avant. Les utilisateurs ayant le niveau de privilège 15 sont également concernés par le paramètre de verrouillage. Commandes nouvelles ou modifiées : **aaa local authentication attempts max-fail** , **show aaa local user**
Invite de modification du mot de passe SSH et Telnet	9.17(1)	La première fois qu'un utilisateur local se connecte à l'ASA à l'aide de SSH ou de Telnet, il est invité à changer de mot de passe. Il sera également invité à se connecter pour la première fois après qu'un administrateur aura modifié son mot de passe. Si l'ASA se recharge, les utilisateurs ne seront pas invités, même s'il s'agit de leur première connexion. Notez que tout service qui utilise la base de données des utilisateurs locale, comme VPN, devra également utiliser le nouveau mot de passe s'il a été modifié lors d'une connexion SSH ou Telnet. Commandes nouvelles ou modifiées : **show aaa local user**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de la sécurité SSH	9.16(1)	SSH prend désormais en charge les améliorations de sécurité suivantes : • Format de clé d'hôte : **crypto key generate** {**eddsa** | **ecdsa**}. En plus de RSA, nous avons ajouté la prise en charge des clés d'hôte EdDSA et ECDSA. L'ASA essaie d'utiliser les clés dans l'ordre suivant, si elles existent : EdDSA, ECDSAA, puis RSA. Si vous configurez explicitement l'ASA pour utiliser la clé RSA avec la commande **ssh key-exchange hostkey rsa**, vous devez générer une clé de 2 048 bits ou plus. Pour des raisons de compatibilité avec les mises à niveau, l'ASA utilisera des clés hôtes RSA de plus petite taille uniquement lorsque le paramètre par défaut de la clé hôte est utilisé. La prise en charge de RSA sera supprimée dans une version ultérieure. • Algorithmes d'échange de clés : **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • Algorithmes de chiffrement : **ssh cipher encryption chacha20-poly1305@openssh.com** • La version 1 de SSH n'est plus prise en charge. La commande **ssh version** est supprimée. Commandes nouvelles ou modifiées : **crypto key generate eddsa**, **crypto key zeroize eddsa**, **show crypto key mypubkey**, **ssh cipher encryption chacha20-poly1305@openssh.com**, **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**}, **ssh key-exchange hostkey**, **ssh version**
Accès de gestion pour SNMP	9.14(2)	Lors de la configuration de l'accès de gestion sur un tunnel VPN, incluez l'adresse IP de l'interface externe dans la liste d'accès de la carte cryptographique dans le cadre de la configuration du VPN pour sécuriser l'interrogation SNMP sur un VPN de site à site.
Paramètre de délai d'inactivité HTTPS	9.14(1)	Vous pouvez maintenant définir le délai d'inactivité pour toutes les connexions HTTPS à l'ASA, y compris ASDM, WebVPN et d'autres clients. Auparavant, avec la commande **http server idle-timeout**, vous pouviez uniquement définir le délai d'inactivité d'ASDM. Si vous définissez les deux délais, la nouvelle commande prévaut. Commandes nouvelles ou modifiées : **http connection idle-timeout**
Le chiffrement SSH est désormais répertorié (de la sécurité la plus haute à la plus basse) pour les listes prédéfinies	9.13(1)	Le chiffrement SSH est désormais répertorié (de la sécurité la plus haute à la sécurité la plus basse) pour les listes prédéfinies (comme moyen ou élevé). Dans les versions précédentes, il était répertorié du niveau le plus bas au plus élevé, ce qui signifie qu'un chiffrement à faible sécurité serait proposé avant un chiffrement à sécurité élevée. Commandes nouvelles ou modifiées : **ssh cipher encryption**

Nom de la caractéristique	Versions de plateforme	Description
La définition du mode d'échange de clés SSH est limitée au contexte d'administration	9.12(2)	Vous devez définir l'échange de clés SSH dans le contexte d'administration; ce paramètre est hérité par tous les autres contextes. Commandes nouvelles ou modifiées : **ssh key-exchange**
Le changement de mot de passe **enable** est maintenant requis lors de la connexion	9.12(1)	Le mot de passe par défaut **enable** est vide. Lorsque vous essayez d'accéder en mode d'exécution privilégié sur l'ASA, vous devez désormais modifier le mot de passe pour une valeur de 3 caractères ou plus. Vous ne pouvez pas le garder vide. La commande **no enable password** n'est plus prise en charge. Au niveau de l'interface de ligne de commande, vous pouvez accéder au mode d'exécution privilégié à l'aide des commandes **enable**, **login** (avec un utilisateur de niveau de privilège 2+), ou d'une session SSH ou Telnet lorsque vous activez **aaa authorization exec auto-enable**. Toutes ces méthodes nécessitent que vous définissiez le mot de passe d'activation. Cette exigence de changement de mot de passe n'est pas appliquée pour les connexions ASDM. Dans ASDM, par défaut, vous pouvez vous connecter sans nom d'utilisateur et avec le mot de passe **enable**. Commandes nouvelles ou modifiées : **enable password**
Limitation configurable des sessions d'administration	9.12(1)	Vous pouvez configurer le nombre maximum de sessions administratives agrégées, par utilisateur et par protocole. Auparavant, vous pouviez configurer uniquement le nombre agrégé de sessions. Cette fonctionnalité n'influe pas sur les sessions de console. Notez qu'en mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions HTTPS, où le maximum est fixé à 5 sessions. La commande **quota management-session** n'est également plus acceptée dans la configuration système et est plutôt disponible dans la configuration du contexte. Le nombre maximum de sessions agrégées est désormais de 15; si vous avez configuré 0 (illimité) ou 16+, lors de la mise à niveau, la valeur passe à 15. Commandes nouvelles/modifiées : **quota management-session**, **show quota management-session**
Notifications pour les modifications du niveau de privilège d'administration	9.12(1)	Lorsque vous vous authentifiez pour activer l'accès (**aaa authentication enable console**) ou autorisez directement l'accès EXEC privilégié (**aaa authorization exec auto-enable**), l'ASA informe désormais les utilisateurs si le niveau d'accès qui leur a été attribué a changé depuis leur dernière connexion. Commandes nouvelles ou modifiées : **show aaa login-history**

Nom de la caractéristique	Versions de plateforme	Description
Sécurité SSH renforcée	9.12(1)	Consultez les améliorations de sécurité SSH suivantes : • Prise en charge de l'échange de clés SHA256, groupe Diffie-Hellman 14. Ce paramètre est désormais la valeur par défaut. L'ancienne valeur par défaut était le groupe 1 SHA1. • Prise en charge du chiffrement d'intégrité HMAC-SHA256. La valeur par défaut est désormais l'ensemble de chiffrements à haute sécurité (hmac-sha2-256 uniquement). L'ancienne valeur par défaut était l'ensemble moyen. Commandes nouvelles ou modifiées : **ssh cipher integrity** , **ssh key-exchange group dh-group14-sha256**
Autoriser les clients HTTPS non basés sur le navigateur à accéder à l'ASA	9.12(1)	Vous pouvez autoriser les clients HTTPS non basés sur le navigateur à accéder aux services HTTPS sur l'ASA. Par défaut, ASDM, CSM et l'API REST sont autorisés. Commandes nouvelles ou modifiées : **http server basic-auth-client**
La paire de clés RSA prend en charge les clés de 3 072 bits	9.9(2)	Vous pouvez maintenant définir la taille du module à 3 072. Commande nouvelle ou modifiée : **crypto key generate rsa modulus**
Accès de gestion du VPN sur les interfaces virtuelles pontées (BVI)	9.9(2)	Vous pouvez maintenant activer des services de gestion, tels que **telnet**, **http** et **ssh**, sur une BVI si le paramètre **management-access** du VPN a été activé sur cette BVI. Pour l'accès de gestion non VPN, vous devez continuer à configurer ces services sur les interfaces membres du groupe de ponts. Commandes nouvelles ou modifiées : **https**, **telnet**, **ssh**, **management-access**
La version 1 de SSH est obsolète	9.9(1)	La version 1 de SSH est obsolète et sera supprimée dans une version ultérieure. Le paramètre par défaut est passé de SSH v1 et v2 à SSH v2. Commandes nouvelles ou modifiées : **ssh version**

Nom de la caractéristique	Versions de plateforme	Description
Authentification distincte pour les utilisateurs disposant d'une authentification par clé publique SSH et les utilisateurs disposant de mots de passe	9.6(3)/9.8(1)	Dans les versions antérieures à 9.6(2), vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer explicitement l'authentification SSH AAA avec la base de données des utilisateurs locale (**aaa authentication ssh console LOCAL**). Dans 9.6(2), l'ASA vous a demandé d'activer explicitement l'authentification SSH AAA. Dans cette version, vous n'avez plus à activer explicitement l'authentification SSH AAA; lorsque vous configurez la commande **ssh authentication** pour un utilisateur, l'authentification locale est activée par défaut pour les utilisateurs avec ce type d'authentification. De plus, lorsque vous configurez explicitement l'authentification SSH AAA, cette configuration s'applique uniquement aux noms d'utilisateur avec *mots de passe*, et vous pouvez utiliser n'importe quel type de serveur AAA (**aaa authentication ssh console radius_1**, par exemple). Par exemple, certains utilisateurs peuvent utiliser l'authentification par clé publique à l'aide de la base de données locale et d'autres utilisateurs peuvent utiliser des mots de passe avec RADIUS. Nous n'avons pas modifié de commandes.
Historique de connexion	9.8(1)	Par défaut, l'historique de connexion est enregistré pendant 90 jours. Vous pouvez désactiver cette fonctionnalité ou modifier la durée, jusqu'à 365 jours. Cette fonctionnalité s'applique uniquement aux noms d'utilisateur dans la base de données locale lorsque vous activez l'authentification AAA locale pour une ou plusieurs des méthodes de gestion (SSH, ASDM, Telnet, etc.). Nous avons introduit les commandes suivantes : **aaa authentication login-history, show aaa login-history**
Application de la politique de mot de passe pour interdire la réutilisation des mots de passe et l'utilisation d'un mot de passe correspondant à un nom d'utilisateur	9.8(1)	Vous pouvez désormais interdire la réutilisation des mots de passe précédents pour un maximum de 7 générations, et vous pouvez également interdire l'utilisation d'un mot de passe correspondant à un nom d'utilisateur. Nous avons introduit les commandes suivantes : **password-history, password-policy reuse-interval, password-policy username-check**
Mode du serveur SSL ASA correspondant à ASDM	9.6(2)	Pour un utilisateur ASDM qui s'authentifie avec un certificat, vous pouvez désormais exiger que le certificat corresponde à une carte de certificat. Nous avons modifié la commande suivante : **http authentication-certificate match**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de l'authentification par clé publique SSH	9.6(2)	Dans les versions antérieures, vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer également l'authentification SSH AAA avec la base de données d'utilisateurs locale (**aaa authentication ssh console LOCAL**). La configuration est désormais modifiée de manière à ce que vous deviez explicitement activer l'authentification SSH AAA. Pour empêcher les utilisateurs d'utiliser un mot de passe au lieu de la clé privée, vous pouvez désormais créer un nom d'utilisateur sans mot de passe défini. Nous avons modifié les commandes suivantes : **ssh authentication, username**
Autorisation de gestion ASDM	9.4(1)	Vous pouvez désormais configurer l'autorisation de gestion séparément pour l'accès HTTP par rapport à l'accès Telnet et SSH. Nous avons introduit la commande suivante : **aaa authorization http console**
Nom d'utilisateur ASDM dans la configuration du certificat	9.4(1)	Lorsque vous activez l'authentification par certificat ASDM (**http authentication-certificate**), vous pouvez configurer la façon dont ASDM extrait le nom d'utilisateur du certificat; vous pouvez également activer le préremplissage du nom d'utilisateur à l'invite de connexion. Nous avons introduit la commande suivante : **http username-from-certificate**
Authentification par mot de passe à usage unique améliorée	9.2(1)	Les administrateurs qui disposent de privilèges d'autorisation suffisants peuvent passer en mode d'exécution privilégié en saisissant une seule fois leurs informations d'authentification. L'option **auto-enable** a été ajoutée à la commande **aaa authorization exec**. Nous avons modifié la commande suivante : **aaa authorization exec**.
Prise en charge de la redirection HTTP pour IPV6	9.1(7)/9.6(1)	Lorsque vous activez la redirection HTTP vers HTTPS pour l'accès ASDM ou le SSL VPN sans client, vous pouvez désormais rediriger le trafic envoyé par vers l'adresse IPv6. Nous avons ajouté des fonctionnalités à la commande suivante : **http redirect**

Nom de la caractéristique	Versions de plateforme	Description
Chiffrement SSH et d'intégrité configurables	9.1(7)9.4(3)9.5(3)9.6(1)	Les utilisateurs peuvent sélectionner des modes de chiffrement lors de la gestion du chiffrement SSH et peuvent configurer le HMAC et le chiffrement pour divers algorithmes d'échange de clés. Vous souhaiterez peut-être modifier les chiffres pour qu'ils soient plus ou moins stricts, selon votre application. Notez que la performance de la copie sécurisée dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier les chiffres proposés, utilisez **ssh cipher encryption custom aes128-cbc**, par exemple. Nous avons introduit les commandes suivantes : **ssh cipher encryption, ssh cipher integrity**.
Chiffrement AES-CTR pour SSH	9.1(2)	La mise en œuvre du serveur SSH dans l'ASA prend désormais en charge le chiffrement en mode AES-CTR.
Intervalle de renouvellement SSH amélioré	9.1(2)	Une connexion SSH est renouvelée après 60 minutes de connexion ou 1 Go de trafic de données. Nous avons introduit la commande suivante : **show ssh sessions detail**.
Pour l'ASASM en mode de contexte multiple, prenez en charge l'authentification Telnet et de la console virtuelle à partir du commutateur.	8.5(1)	Bien que la connexion à l'ASASM à partir du commutateur en mode de contexte multiple se connecte à l'espace d'exécution du système, vous pouvez configurer l'authentification dans le contexte d'administration pour régir ces connexions.
Prise en charge de la politique de mot de passe administrateur lors de l'utilisation de la base de données locale	8.4(4.1), 9.1(2)	Lorsque vous configurez l'authentification pour l'accès à l'interface de ligne de commande ou à ASDM à l'aide de la base de données locale, vous pouvez configurer une politique de mot de passe qui oblige un utilisateur à changer de mot de passe après une durée spécifiée et qui exige également des normes de mot de passe telles qu'une longueur minimum et le nombre minimum de modifications de caractères. Nous avons introduit les commandes suivantes : **change-password**, **password-policy lifetime**, **password-policy minimum changes**, **password-policy minimum-length**, **password-policy minimum-lowercase**, **password-policy minimum-uppercase**, **password-policy minimum-numeric**, **password-policy minimum-special**, **password-policy authenticate enable**, **clear configure password-policy**, **show running-config password-policy**.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de l'authentification par clé publique SSH	8.4(4.1), 9.1(2)	Vous pouvez activer l'authentification par clé publique pour les connexions SSH à l'ASA par utilisateur. Vous pouvez spécifier une clé formatée de fichier de clé publique (PKF) ou une clé Base64. La clé PKF peut comporter jusqu'à 4 096 bits. Utilisez le format PKF pour les clés qui sont trop grandes pour la prise en charge ASA du format Base64 (jusqu'à 2 048 bits). Nous avons introduit les commandes suivantes : **ssh authentication**. *Le format de clé PKF est uniquement pris en charge dans la version 9.1(2) et les versions ultérieures.*
Prise en charge du groupe Diffie-Hellman 14 pour l'échange de clés SSH	8.4(4.1), 9.1(2)	La prise en charge du groupe Diffie-Hellman 14 pour l'échange de clés SSH a été ajoutée. Auparavant, seul le groupe 1 était pris en charge. Nous avons introduit la commande suivante : **ssh key-exchange**.
Prise en charge d'un nombre maximum de sessions de gestion	8.4(4.1), 9.1(2)	Vous pouvez définir le nombre maximum de sessions ASDM, SSH et Telnet simultanées. Nous avons ajouté les commandes suivantes : **quota management-session**, **show running-config quota management-session**, **show quota management-session**.
Sécurité SSH améliorée; le nom d'utilisateur SSH par défaut n'est plus pris en charge.	8.4(2)	À partir de la version 8.4(2), vous ne pouvez plus vous connecter à l'ASA à l'aide de SSH avec le nom d'utilisateur pix ou asa et le mot de passe de connexion. Pour utiliser SSH, vous devez configurer l'authentification AAA à l'aide de la commande **aaa authentication ssh console LOCAL** (interface de ligne de commande) ou Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authentication (ASDM) (Authentification (ASDM)); puis définissez un utilisateur local en saisissant la commande **username** (interface de ligne de commande) ou en sélectionnant Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (ASDM) (Comptes d'utilisateurs (ASDM)). Si vous souhaitez utiliser un serveur AAA pour l'authentification au lieu de la base de données locale, nous vous conseillons de configurer également l'authentification locale comme méthode de sauvegarde.

Nom de la caractéristique	Versions de plateforme	Description
Accès de gestion	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les commandes suivantes : **show running-config all privilege all**, **show running-config privilege level**, **show running-config privilege command**, **telnet**, **telnet timeout**, **ssh**, **ssh timeout**, **http**, **http server enable**, **asdm image disk, banner**, **console timeout**, **icmp**, **ipv6 icmp**, **management access**, **aaa authentication console**, **aaa authentication enable console**, **aaa authentication telnet | ssh console**, **service-type**, **login**, **privilege**, **aaa authentication exec authentication-server**, **aaa authentication command LOCAL**, **aaa accounting serial | telnet | ssh | enable console**, **show curpriv**, **aaa accounting command privilege**.



CHAPITRE 44

Logiciels et configurations

Ce chapitre décrit comment gérer le logiciel et les configurations ASA.

- Mettre à niveau le logiciel, à la page 1331
- Charger une image à l'aide de ROMMON (ISA 3000), à la page 1331
- Mettre à niveau l'image ROMMON : ISA 3000, à la page 1333
- Rétrograder votre logiciel, à la page 1334
- Gérer les fichiers, à la page 1340
- Définir l'image ASA, ASDM et la configuration de démarrage, à la page 1350
- Sauvegarde et restauration de configurations ou d'autres fichiers, à la page 1353
- Échange à chaud d'un SSD sur Cisco Secure Firewall, à la page 1371
- Historique des logiciels et des configurations, à la page 1373

Mettre à niveau le logiciel

Consultez le Guide de mise à niveau de Cisco ASA pour accéder aux procédures de mise à niveau complètes.

Charger une image à l'aide de ROMMON (ISA 3000)

Pour charger une image logicielle sur un ASA en mode ROMMON à l'aide de TFTP, procédez comme suit.

Procédure

Étape 1 Connectez-vous au port de la console de l'ASA en suivant les instructions de Accéder à la console de l'ISA 3000, à la page 11.

Étape 2 Mettez l'ASA hors tension, puis rallumez-le.

Étape 3 Pendant le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à passer en mode ROMMON.

Étape 4 En mode ROMMON, définissez les paramètres d'interface avec l'ASA, notamment l'adresse IP, l'adresse du serveur TFTP, l'adresse de la passerelle, le fichier d'image logicielle et le port, comme suit :

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
```

```
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

Remarque
Assurez-vous que la connexion au réseau est déjà établie.

Sur les plateformes ASA 5506-X, ASA 5508-X, ASA 5516-X et ISA 3000, la commande **interface** ne fonctionne pas, ce qui oblige à utiliser l'interface Management 1/1 pour la récupération TFTP.

Étape 5 Validez les paramètres :

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

Étape 6 Envoyez un message Ping au serveur TFTP :

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

Étape 7 Enregistrez les paramètres réseau pour une utilisation ultérieure :

```
rommon #8> sync
Updating NVRAM Parameters...
```

Étape 8 Chargez l'image logicielle :

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016
```

```
Loading...
```

Une fois l'image logicielle chargée, l'ASA quitte automatiquement le mode ROMMON.

Étape 9 Le démarrage de l'ASA en mode ROMMON ne permet pas de conserver l'image du système après un rechargement. Vous devez donc télécharger l'image dans la mémoire flash. Consultez le Guide de mise à niveau de Cisco ASA pour accéder aux procédures de mise à niveau complètes.

Mettre à niveau l'image ROMMON : ISA 3000

Pour les ISA 3000, procédez comme suit afin de mettre à niveau l'image ROMMON. Pour les modèles ASA, vous devez avoir installé la version 1.1.8 ou toute version ultérieure de ROMMON sur votre système. Nous vous recommandons d'effectuer la mise à niveau vers la dernière version.

Seule une mise à niveau vers une nouvelle version est possible; la rétrogradation n'est pas prise en charge.

Mise en garde La ISA 3000 prend deux fois plus de temps que pour les versions précédentes (environ 15 minutes). **N'éteignez pas** l'appareil pendant la mise à niveau. Si la mise à niveau prend plus de 30 minutes ou si elle échoue, contactez l'assistance technique de Cisco. **N'éteignez pas** l'appareil et ne le réinitialisez pas.

Avant de commencer

Procurez-vous la nouvelle image ROMMON sur Cisco.com et enregistrez-la sur un serveur pour ensuite la copier sur l'ASA. L'ASA prend en charge les serveurs FTP, TFTP, SCP, HTTP(S) et SMB. Téléchargez l'image de :

- ISA 3000 : https://software.cisco.com/download/home/286288493/type

Procédure

Étape 1 Copiez l'image ROMMON sur la mémoire flash de l'ASA. Cette procédure illustre la commande « copy FTP ». Entrez **copy ?** pour la syntaxe appropriée pour les autres types de serveurs.

copy ftp://[*noms d'utilisateur***:***mot de passe***@**]*server_ip***/asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

Étape 2 Pour connaître la version installée, entrez la commande **show module** et consultez la version du pare-feu (FW) dans la sortie du module 1 du tableau des plages d'adresses MAC :

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

Étape 3 Procédez à la mise à niveau de l'image ROMMON :

upgrade rommon disk0:asa5500-firmware-*XXXX*.SPA

Exemple :

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

Étape 4 Lorsque vous y êtes invité, appuyez sur Confirmer pour recharger l'ASA.

L'ASA met à niveau l'image ROMMON, puis recharge le système d'exploitation.

Rétrograder votre logiciel

Dans de nombreux cas, vous pouvez rétrograder votre logiciel ASA et restaurer une configuration de sauvegarde à partir de la version de logiciel précédemment installée. La méthode de rétrogradation dépend de votre plateforme ASA.

Directives et limites en matière de rétrogradation

Consultez les consignes suivantes avant la rétrogradation :

- **Il n'y a pas de prise en charge officielle de la rétrogradation sans temps d'arrêt pour la mise en grappe**. Cependant la rétrogradation sans temps d'arrêt fonctionnera dans certains cas. Consultez les problèmes connus suivants relatifs à la rétrogradation. Veuillez noter que d'autres problèmes peuvent vous obliger à recharger vos unités de grappe, ce qui entraînera un temps d'arrêt.

- **La rétrogradation à une version antérieure à la version 9.9(1) avec mise en grappe**: la version 9.9(1) et les versions ultérieures inclut une amélioration de la distribution des sauvegardes. Si vous avez au moins 3 unités dans la grappe, vous devez effectuer les étapes suivantes :

  1. Supprimez toutes les unités secondaires de la grappe (pour que celle-ci ne se compose que de l'unité principale).
  2. Rétrogradez une unité secondaire et réintégrez-la à la grappe.
  3. Désactivez la mise en grappe sur l'unité principale, rétrogradez-la et réintégrez-la à la grappe.
  4. Rétrogradez les unités secondaires restantes et joignez-les à la grappe, une à la fois.

- **Rétrograder à une version antérieure à la version 9.9(1) lorsque vous activez la redondance du site en grappe** : vous devez désactiver la redondance de site si vous souhaitez effectuer une rétrogradation (ou si vous souhaitez ajouter à une grappe une unité dont la version est antérieure à la version 9.9(1)). Sinon, vous constaterez des effets secondaires, par exemple des flux de transfert fictifs sur l'unité exécutant l'ancienne version.
- **Rétrogradation à partir de la version 9.8(1) avec mise en grappe et carte de chiffrement** : il n'y a pas de prise en charge de la rétrogradation sans temps d'arrêt à partir de la version 9.8(1) lorsqu'une carte de chiffrement est configurée. Vous devez effacer la configuration de la carte de chiffrement avant la rétrogradation, puis réappliquer la configuration après la rétrogradation.
- **Rétrograder de la version 9.8(1) avec un contrôle d'intégrité de l'unité de mise en grappe défini sur 0,3 à 0,7 seconde** : si vous rétrogradez votre logiciel ASA après avoir défini le délai de rétention sur 0,3–0,7 (**health-check holdtime**), ce paramètre reviendra à la valeur par défaut de 3 secondes, car le nouveau paramètre n'est pas pris en charge.
- **Rétrogradation à partir de la version 9.5(2) ou d'une version ultérieure à la version 9.5(1) ou une version antérieure avec mise en grappe (CSCuv82933) :** il n'y a pas de prise en charge de la rétrogradation sans temps d'arrêt à partir de la version 9.5(2). Vous devez recharger toutes les unités à peu près en même temps afin qu'un nouveau cluster se forme lorsque les unités sont de nouveau en ligne. Si vous attendez pour recharger les unités de manière séquentielle, elles ne pourront pas former de grappe.
- **Rétrogradation à partir de la version 9.2(1) ou d'une version ultérieure à la version 9.1 ou une version antérieure avec mise en grappe** : la rétrogradation sans temps d'arrêt n'est pas prise en charge.

- **Problème de rétrogradation de la version 9.18 ou ultérieure** : il y a un changement de comportement dans la version 9.18 où la commande **access-group** sera répertoriée avant ses commandes **access-list**. Si vous effectuez une rétrogradation, la commande **access-group** sera rejetée, car elle n'a pas encore chargé les commandes **access-list**. Ce résultat se produit même si vous avez précédemment activé la commande **forward-reference enable**, car cette commande est maintenant supprimée. Avant de procéder à la rétrogradation, assurez-vous de copier toutes les commandes **access-group** manuellement, puis après la rétrogradation, saisissez-les de nouveau.
- **Problème de rétrogradation du Firepower 2100 en mode plateforme à partir de la version 9.13/9.14 à la version 9.12 ou à une version antérieure** : pour un Firepower 2100 disposant d'une nouvelle installation de la version 9.13 ou 9.14 que vous avez convertie en mode plateforme : si vous rétrogradez le périphérique à la version 9.12 ou à une version antérieure, vous ne pourrez pas configurer de nouvelles interfaces ni modifier des interfaces existantes dans FXOS (notez que la version 9.12 et les versions antérieures ne prennent en charge que le mode plateforme). Vous devez soit restaurer votre version à la

version 9.13 ou à une version ultérieure, soit effacer votre configuration à l'aide de la commande de configuration d'effacement FXOS. Ce problème ne se produit pas si vous avez initialement effectué une mise à niveau vers la version 9.13 ou 9.14 à partir d'une version antérieure. Seules les nouvelles installations sont concernées, comme un nouveau périphérique ou un périphérique recréé. (CSCvr19755)

- **Rétrogradation de la version 9.10(1) pour les licences Smart** : en raison de modifications dans l'agent Smart, si vous effectuez une rétrogradation, vous devez réenregistrer votre périphérique auprès de Cisco Smart Software Manager. Le nouvel agent Smart utilise un fichier chiffré. Vous devez donc vous réenregistrer pour utiliser un fichier non chiffré requis par l'ancien agent Smart.
- **Rétrograder à la version 9.5 ou à une version antérieure avec des mots de passe utilisant le hachage PBCDF2 (Password-Based Key Derivation Function 2)** : les versions antérieures à la version 9.6 ne prennent pas en charge le hachage PBKDF2. Dans la version 9.6(1), les mots de passe **enable** et **username** de plus de 32 caractères utilisent le hachage PBCDF2. Dans la version 9.7(1), les nouveaux mots de passe de toutes les longueurs utilisent le hachage PBCDF2 (les mots de passe existants continuent d'utiliser le hachage MD5). Si vous effectuez une rétrogradation, le mot de passe de **enable** revient à la valeur par défaut (c'est-à-dire vide). Les noms d'utilisateur ne seront pas analysés correctement, et les commandes **username** seront supprimées. Vous devez recréer vos utilisateurs locaux.
- **Rétrograder à partir de la version 9.5(2.200) pour le ASA virtuel** : le ASA virtuel ne conserve pas l'état d'enregistrement de la licence. Vous devez vous réenregistrer à l'aide de la commande **license smart register idtoken id_token force** (pour ASDM : consultez la page **Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Smart Licensing (Licences Smart)** et utilisez l'option **Force registration** (Forcer l'enregistrement)); obtenez le jeton d'identification auprès de Smart Software Manager.
- **Les tunnels VPN sont répliqués sur l'unité de secours même si cette dernière exécute une version du logiciel qui ne prend pas en charge la suite de chiffrement que le tunnel d'origine a négociée.** Ce scénario se produit lors de la rétrogradation. Dans ce cas, déconnectez votre connexion VPN et reconnectez-vous.

Configuration incompatible supprimée après la rétrogradation

Lorsque vous effectuez une rétrogradation à une ancienne version, les commandes qui ont été introduites dans les versions ultérieures seront supprimées de la configuration. Il n'existe aucun moyen automatisé de vérifier la configuration par rapport à la version cible avant de procéder à la rétrogradation. Vous pouvez découvrir quand de nouvelles commandes ont été ajoutées dans les nouvelles fonctionnalités d'ASA par version.

Vous pouvez afficher les commandes rejetées *après* avoir effectué une rétrogradation en utilisant la commande **show startup-config errors**. Si vous pouvez rétrograder un périphérique de laboratoire, vous pouvez prévisualiser les effets en utilisant cette commande avant de rétrograder un périphérique de production.

Dans certains cas, l'ASA migre automatiquement les commandes vers de nouveaux formulaires lors de la mise à niveau. Ainsi, selon votre version, même si vous n'avez pas configuré manuellement de nouvelles commandes, la rétrogradation peut être influencée par les migrations de configuration. Nous vous recommandons de sauvegarder votre ancienne configuration logicielle afin de pouvoir l'utiliser lors de la rétrogradation. Dans le cas d'une mise à niveau vers la version 8.3, une sauvegarde est automatiquement créée (<old_version>_startup_cfg.sav). Les autres migrations ne créent pas de sauvegardes. Consultez les « Directives et migrations propres à la version » dans le guide de mise à niveau d'ASA pour en savoir plus sur les migrations automatiques des commandes qui pourraient avoir une incidence sur la rétrogradation.

Consultez également les problèmes de rétrogradation connus dans Directives et limites en matière de rétrogradation, à la page 1334.

Par exemple, un ASA utilisant la version 9.8(2) inclut les commandes suivantes :

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

Lorsque vous rétrogradez le périphérique à la version 9.0(4), les erreurs suivantes s'afficheront au démarrage :

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
                                   ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                               ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
                                     ^
ERROR: % Invalid input detected at '^' marker.
```

Dans cet exemple, la prise en charge de **sctp** dans la commande **access-list étendue** a été ajoutée dans la version 9.5(2), la prise en charge de **pbkdf2** dans la commande **username** a été ajoutée dans la version 9.6(1) et la prise en charge de **engineID** dans la commande **snmp-server user** a été ajouté dans la version 9.5(3).

Rétrograder l'appareil ASA

Vous pouvez rétrograder la version du logiciel de l'ASA en définissant la version de l'ASA sur l'ancienne version, en restaurant la configuration de sauvegarde dans la configuration de démarrage, puis en la rechargeant. Cette procédure s'applique aux modèles suivants :

- Firepower 1000
- Secure Firewall 1200
- Firepower de la série 2100
- Secure Firewall 3100
- Secure Firewall 4200

Avant de commencer

Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration. Si vous ne restaurez pas l'ancienne configuration, vous risquez d'avoir des commandes incompatibles représentant des fonctionnalités nouvelles ou modifiées. Toute nouvelle commande sera rejetée lorsque vous chargerez l'ancienne version du logiciel.

Procédure

Étape 1 Chargez l'ancienne version du logiciel ASA en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe. Dans ce cas, précisez l'ancienne version d'ASA au lieu d'une nouvelle version. **Important :** Ne rechargez *pas* encore l'ASA.

Étape 2 Au niveau de l'interface de ligne de commande de l'ASA, copiez la configuration de l'ASA de secours dans la configuration de démarrage. Pour le basculement, effectuez cette étape sur l'unité active. Cette étape réplique la commande sur l'unité de secours.

copy *ancienne_url_de_configuration* **startup-config**

Il est important que vous n'enregistriez pas la configuration en cours dans la configuration de démarrage à l'aide de **write memory**; cette commande remplacera votre configuration de sauvegarde.

Exemple :

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

Étape 3 Rechargez l'ASA.

Interface de ligne de commande ASA

reload

ASDM

Choisissez **Tools (Outils)** > **System Reload (Rechargement du système)**.

Rétrograder le Firepower 2100 en mode plateforme

Vous pouvez rétrograder la version du logiciel de l'ASA en restaurant la configuration de sauvegarde à la configuration de lancement, en réglant la version de l'ASA à l'ancienne version, puis en rechargeant l'unité.

Avant de commencer

Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration. Si vous ne restaurez pas l'ancienne configuration, vous risquez d'avoir des commandes incompatibles représentant des fonctionnalités nouvelles ou modifiées. Toute nouvelle commande sera rejetée lorsque vous chargerez l'ancienne version du logiciel.

Procédure

Étape 1 Au niveau de l'interface de ligne de commande de l'ASA, copiez la configuration de l'ASA de secours dans la configuration de démarrage. Pour le basculement, effectuez cette étape sur l'unité active. Cette étape réplique la commande sur l'unité de secours.

copy *ancienne_url_de_configuration* **startup-config**

Il est important que vous n'enregistriez pas la configuration en cours dans la configuration de démarrage à l'aide de **write memory**; cette commande remplacera votre configuration de sauvegarde.

Exemple :

```
ciscoasa# copy disk0:/9.12.4_cfg.sav startup-config
```

Étape 2 Dans FXOS, utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour utiliser l'ancienne version du logiciel ASA en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe. Dans ce cas, précisez l'ancienne version d'ASA au lieu d'une nouvelle version.

Rétrograder le Firepower 4100/9300

Vous pouvez rétrograder la version du logiciel de l'ASA en restaurant la configuration de sauvegarde à la configuration de lancement, en réglant la version de l'ASA à l'ancienne version, puis en rechargeant l'unité.

Avant de commencer

- Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration. Si vous ne restaurez pas l'ancienne configuration, vous risquez d'avoir des commandes incompatibles représentant des fonctionnalités nouvelles ou modifiées. Toute nouvelle commande sera rejetée lorsque vous chargerez l'ancienne version du logiciel.
- Assurez-vous que l'ancienne version de l'ASA est compatible avec la version de FXOS actuelle. Si ce n'est pas le cas, rétrogradez FXOS en premier lieu avant de restaurer l'ancienne configuration ASA. Assurez-vous que l'instance rétrogradée de FXOS est également compatible avec la version d'ASA actuelle (avant de la rétrograder). Si vous ne parvenez pas à assurer la compatibilité, nous vous conseillons de ne pas procéder à une rétrogradation.

Procédure

Étape 1 Au niveau de l'interface de ligne de commande de l'ASA, copiez la configuration de l'ASA de secours dans la configuration de démarrage. Pour le basculement ou la mise en grappe, effectuez cette étape sur l'unité active/de contrôle. Cette étape réplique la commande sur les unités de secours/de données.

copy *ancienne_url_de_configuration* **startup-config**

Il est important que vous n'enregistriez pas la configuration en cours dans la configuration de démarrage à l'aide de **write memory**; cette commande remplacera votre configuration de sauvegarde.

Exemple :

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

Étape 2 Dans FXOS, utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour utiliser l'ancienne version du logiciel ASA en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe. Dans ce cas, précisez l'ancienne version d'ASA au lieu d'une nouvelle version.

Étape 3 Si vous rétrogradez également FXOS, utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour définir l'ancienne version du logiciel FXOS pour qu'elle soit la version actuelle en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe.

Rétrograder l'ISA 3000

La fonctionnalité de rétrogradation fournit un raccourci pour effectuer les fonctions suivantes sur les modèles ISA 3000 :

- Effacement de la configuration de l'image de démarrage (**clear configure boot**).
- Définition de l'image de démarrage comme étant l'ancienne image (**boot system**).
- (Facultatif) Entrée d'une nouvelle clé d'activation (**activation-key**).
- Enregistrement de la configuration en cours pour le démarrage (**write memory**). Cette opération définit la variable d'environnement BOOT sur l'ancienne image, de sorte que lorsque vous rechargez, l'ancienne image est chargée.
- Copie de l'ancienne sauvegarde de configuration dans la configuration de démarrage (**copy** *ancienne_url_de_configuration* **startup-config**).
- Rechargement (**reload**).

Avant de commencer

- Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration.

Procédure

rétrogradez le logiciel et restaurez l'ancienne configuration.

downgrade [**/noconfirm**] *ancienne_url_d_image ancienne_url_de_configuration* [**activation-key** *ancienne_clé*]

Exemple :

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

L'option **/noconfirm** est rétrogradée sans invite. L'*url_de_l_image* est le chemin d'accès à l'ancienne image sur disk0, disk1, tftp, ftp ou smb. L'*ancienne_url_de_configuration* est le chemin d'accès à la configuration de pré-migration enregistrée. Si vous devez revenir à une clé d'activation antérieure à la version 8.3, vous pouvez saisir l'ancienne clé d'activation.

Gérer les fichiers

Afficher les fichiers dans la mémoire flash

Vous pouvez afficher les fichiers dans la mémoire flash et voir des renseignements sur les fichiers.

Procédure

Étape 1 Affichez les fichiers dans la mémoire flash :

dir [**disk*n*:**]

disk0: est la mémoire interne. D'autres numéros de lecteur représentent un stockage externe tel qu'un lecteur USB, un SSD ou une carte SD.

Exemple :

```
hostname# dir

Directory of disk0:/
500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
```

Étape 2 Affichez des renseignements étendus sur un fichier en particulier :

show file information [path:/]*filename*

Exemple :

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

La taille de fichier répertoriée est à titre d'exemple uniquement.

Le chemin par défaut est le répertoire racine de la mémoire flash interne (disk0:/).

Supprimer des fichiers de la mémoire flash

Vous pouvez supprimer des fichiers de la mémoire flash dont vous n'avez plus besoin.

Procédure

Supprimez un fichier de la mémoire flash :

delete disk*n*: *filename*

disk0: est la mémoire interne. D'autres numéros de lecteur représentent un stockage externe tel qu'un lecteur USB, un SSD ou une carte SD.

Par défaut, le fichier est supprimé du répertoire de travail actuel si vous ne spécifiez pas de chemin. Vous pouvez utiliser des caractères génériques lors de la suppression de fichiers. Vous êtes invité à indiquer le nom de fichier à supprimer, puis vous devez confirmer la suppression.

Effacer le système de fichiers flash

Pour effacer le système de fichiers flash, procédez comme suit.

Procédure

Étape 1 Connectez-vous au port de la console de l'ASA en suivant les instructions deAccéder à la console de l'ISA 3000, à la page 11.

Étape 2 Mettez l'ASA hors tension, puis rallumez-le.

Étape 3 Pendant le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à passer en mode ROMMON.

Étape 4 Saisissez la commande **erase**, qui remplace tous les fichiers et efface le système de fichiers, y compris les fichiers système masqués :

rommon #1> **erase** [**disk0:** | **disk***n***:** | **usb:**]

disk0: est la mémoire interne. Les autres numéros de lecteur représentent le stockage externe. Les modèles plus récents utilisent **usb:** pour le lecteur USB externe.

Configurer l'accès au fichier

L'ASA peut utiliser un client FTP, un client de copie sécurisée ou un client TFTP. Vous pouvez également configurer l'ASA en tant que serveur de copie sécurisée afin de pouvoir utiliser un client de copie sécurisée sur votre ordinateur.

Configurer le mode client FTP

L'ASA peut utiliser FTP pour charger ou télécharger des fichiers image ou des fichiers de configuration vers ou depuis un serveur FTP. En mode FTP passif, le client initie à la fois la connexion de contrôle et la connexion de données. Le serveur, qui est le destinataire de la connexion de données en mode passif, répond par le numéro de port sur lequel il écoute pour la connexion spécifique.

Procédure

Définissez le mode FTP sur passif :

ftp mode passive

Exemple :

```
ciscoasa(config)# ftp mode passive
```

Configurer l'ASA Secure Copy Client

Vous pouvez configurer les paramètres SCP à l'aide de la commande **copy**.

La performance de SCP dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier le chiffrement proposé, utilisez la commande **ssh cipher encryption** le volet; par exemple, **ssh cipher encryption custom aes128-cbc**

Avant de commencer

- La licence ASA doit avoir la licence de cryptage renforcé (3DES/AES) pour prendre en charge les connexions SSH version 2.
- Sauf indication contraire, pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.
- Pour le serveur SCP, activez SSH sur l'ASA conformément à Configurer l'accès SSH, à la page 1275.

Procédure

Étape 1 (Facultatif) L'ASA stocke la clé d'hôte SSH pour chaque serveur SCP auquel elle se connecte. Vous pouvez gérer manuellement les clés si vous le souhaitez.

ssh pubkey-chain [**no**] **server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*}

Exemple :

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:
e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12
```

Pour chaque serveur, vous pouvez spécifier la **key-string** (clé publique) ou le **key-hash** (valeur de hachage) de l'hôte SSH.

La *key_string* est la clé publique RSA codée en Base64 de l'homologue distant. Vous pouvez obtenir la valeur de clé publique à partir d'un client SSH ouvert; c'est-à-dire du fichier .ssh/id_rsa.pub. Après avoir soumis la clé publique codée en Base64, cette clé est ensuite hachée au moyen de SHA-256.

Le **key-hash** {**md5** | **sha256**} *fingerprint* saisit la clé déjà hachée (à l'aide d'une clé MD5 ou SHA-256); par exemple, une clé que vous avez copiée à partir de la sortie de la commande **show**.

Étape 2 (Facultatif) Activez ou désactivez la vérification de la clé d'hôte SSH. Pour le mode de contexte multiple, saisissez cette commande dans le contexte d'administration.

[**no**] **ssh stricthostkeycheck**

Exemple :

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

Par défaut, cette option est activée. Lorsque cette option est activée, vous êtes invité à accepter ou à refuser la clé d'hôte si elle n'est pas déjà stockée sur l'ASA. Lorsque cette option est désactivée, l'ASA accepte automatiquement la clé d'hôte si elle n'a pas été stockée auparavant.

Exemples

L'exemple suivant ajoute une clé d'hôte déjà hachée pour le serveur à l'adresse 10.86.94.170 :

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:
64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

L'exemple suivant ajoute une clé de chaîne d'hôte pour le serveur à l'adresse 10.7.8.9 :

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:
46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

Configurer le chemin du client TFTP pour l'ASA

Le TFTP est un protocole de transfert de fichiers client/serveur simple, qui est décrit dans les RFC 783 et RFC 1350, version 2. Vous pouvez configurer l'ASA en tant que client TFTP afin qu'il puisse copier des fichiers vers ou à partir d'un serveur TFTP. De cette façon, vous pouvez sauvegarder et propager des fichiers de configuration sur plusieurs ASA.

Cette section vous permet de prédéfinir le chemin d'accès à un serveur TFTP afin de ne pas avoir à le saisir dans des commandes telles que **copy** et **configure net**.

Procédure

Prédéfinissez l'adresse du serveur TFTP et le nom de fichier à utiliser avec les commandes **configure net** et **copy** :

tftp-server *interface_name server_ip filename*

Exemple :

```
ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg
ciscoasa(config)# copy tftp: test.cfg

Address or name of remote host [10.1.4.7]?

Source filename [files/config1.cfg]?config2.cfg

Destination filename [test.cfg]?

Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...
```

Vous pouvez remplacer le nom de fichier lorsque vous saisissez la commande; par exemple, lorsque vous utilisez la commande **copy**, vous pouvez tirer parti de l'adresse du serveur TFTP prédéfinie, mais saisir un nom de fichier dans les invites interactives.

Pour la commande **copy**, saisissez **tftp:** pour utiliser la valeur tftp-server au lieu de **tftp://***url*.

Copier un fichier sur l'ASA

Cette section décrit comment copier l'image de l'application, le logiciel ASDM, un fichier de configuration ou tout autre fichier qui doit être téléchargé dans la mémoire flash interne ou externe à partir d'un serveur TFTP, FTP, SMB, HTTP, HTTPS, SCP ou d'un lecteur tel qu'une clé USB.

Directives

- **disk0:** est la mémoire interne. D'autres numéros de lecteur représentent un stockage externe tel qu'un lecteur USB, un SSD ou une carte SD.
- Assurez-vous que le lecteur USB est au format EXT2/3/4 ou VFAT/FAT32.
- Vous ne pouvez pas avoir deux fichiers du même nom, mais avec une casse différente dans le même répertoire de mémoire flash. Par exemple, si vous tentez de télécharger le fichier Config.cfg à un emplacement qui contient le fichier config.cfg, vous recevez le message d'erreur suivant :

```
%Error opening disk0:/Config.cfg (File exists)
```

- Pour le mode de contexte multiple, vous devez être dans l'espace d'exécution du système, sauf si vous configurez le stockage privé (**storage-url private**). Dans un contexte, vous pouvez également copier la configuration de démarrage (voir Copier un fichier dans la configuration de démarrage ou d'exécution, à la page 1348 si vous avez un stockage privé et Sauvegarder une configuration de contexte dans un contexte, à la page 1363), ou une capture. SCP n'est pas pris en charge dans un contexte utilisant la pile CiscoSSH.

Avant de commencer

- Pour utiliser la commande **copy** de l'ASA afin de copier un fichier vers ou depuis un serveur SCP, vous devez :
  - (Pile CiscoSSH uniquement) Activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP à l'aide de la commande **ssh**.
  - Générer une paire de clés (pour les ASA physiques uniquement) à l'aide de la commande **crypto key generate**.

Procédure

Copiez un fichier en utilisant l'un des types de serveur suivants.

- Copiez à partir d'un serveur TFTP :

  copy [**/noconfirm**] [*interface_name*] **tftp:**//*server*[/*path*]/*src_filename* **disk***n***:**/[*path*/]*dest_filename*

  Exemple :

```
ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg

Address or name of remote host [10.1.1.67]?

Source filename [files/context1.cfg]?

Destination filename [context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- Copiez à partir d'un serveur FTP :

  copy [**/noconfirm**] [*interface_name*] **ftp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*src_filename* **disk***n***:**/[*path*/]*dest_filename*

  Exemple :

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg
disk0:/contexts/context1.cfg

Address or name of remote host [10.1.1.67]?

Source username [jcrichton]?
```

```
Source password [aeryn]?

Source filename [files/context1.cfg]?

Destination filename [contexts/context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- Copiez à partir d'un serveur HTTP(S) :

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  Exemple :

```
ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg

Address or name of remote host [10.1.1.67]?

Source username [asun]?

Source password [john]?

Source filename [files/moya.cfg]?

Destination filename [contexts/moya.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- Copiez à partir d'un serveur SMB :

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  Exemple :

```
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- Copiez à partir d'un serveur SCP :

  L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur SCP.

  copy [**/noconfirm**] [*interface_name*]
  scp://[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] **disk***n***:/**[*path/*]*dest_filename*

  Exemple :

```
ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg

Address or name of remote host [10.86.94.170]?
```

```
Source username [pilot]?

Destination filename [test.cfg]?

The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established.
RSA key fingerprint is
<65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19>(SHA256).
Are you sure you want to continue connecting (yes/no)? yes

Please use the following commands to add the hash key to the configuration:
  ssh pubkey-chain
    server 10.86.94.170
      key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19


Password: <type in password>
!!!!!!
6006 bytes copied in 8.160 secs (750 bytes/sec)
```

- Copiez à partir d'une clé USB ou d'un lecteur interne ou externe :

  copy [**/noconfirm**] **disk***n***:/**[*path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  Exemple :

```
ciscoasa# copy /noconfirm disk1:/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

Copier un fichier dans la configuration de démarrage ou d'exécution

Vous pouvez télécharger un fichier texte pour la configuration de démarrage à partir d'un serveur TFTP, FTP, SMB, HTTP(S) ou SCP, ou à partir de la mémoire flash.

Lorsque vous copiez une configuration dans la configuration en cours d'exécution, vous fusionnez les deux configurations. Une fusion ajoute toutes les nouvelles commandes de la nouvelle configuration à la configuration en cours d'exécution. Si les configurations sont identiques, aucune modification ne se produit. Si des commandes sont en conflit ou si des commandes influent sur le fonctionnement de l'ASA, l'effet de la fusion dépend de la commande. Vous pourriez obtenir des erreurs ou des résultats inattendus.

(Facultatif) Spécifiez l'interface par laquelle l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

Dans un contexte en mode de contexte multiple, vous pouvez utiliser cette procédure si vous activez le stockage privé (**storage-url private**). Sans stockage privé, pour télécharger à partir d'un serveur TFTP vers la configuration du contexte en cours d'exécution, utilisez la commande **configure net** . SCP n'est pas pris en charge dans un contexte utilisant la pile CiscoSSH

Procédure

Pour copier un fichier dans la configuration de démarrage ou la configuration en cours d'exécution, saisissez l'une des commandes suivantes pour le serveur de téléchargement approprié :

- Copiez à partir d'un serveur TFTP :

  copy [**/noconfirm**] [*interface_name*] **tftp://***server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config
  ```

- Copiez à partir d'un serveur FTP :

  copy [**/noconfirm**] [*interface_name*] **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config
  ```

- Copiez à partir d'un serveur HTTP(S) :

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config
  ```

- Copiez à partir d'un serveur SMB :

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config
  ```

- Copiez à partir d'un serveur SCP :

  copy [**/noconfirm**] [*interface_name*] **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config
  ```

L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur SCP.

Exemples

Par exemple, pour copier la configuration à partir d'un serveur TFTP, saisissez la commande suivante :

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

Pour copier la configuration à partir d'un serveur FTP, saisissez la commande suivante :

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

Pour copier la configuration à partir d'un serveur HTTP, saisissez la commande suivante :

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

Définir l'image ASA, ASDM et la configuration de démarrage

Si vous avez plus d'une image ASA ou ASDM, vous devez spécifier l'image que vous souhaitez démarrer. Si vous ne définissez pas l'image, l'image de démarrage par défaut est utilisée et cette image peut ne pas être celle prévue. Pour la configuration de démarrage, vous pouvez éventuellement spécifier un fichier dans le système de fichiers visible au lieu d'un répertoire masqué.

Voir les directives suivantes concernant les modèles :

- Châssis Firepower 4100/9300 : les mises à niveau ASA sont gérées par FXOS; vous ne pouvez pas mettre à niveau l'ASA dans le système d'exploitation de l'ASA, donc n'utilisez pas cette procédure pour l'image de l'ASA. Vous pouvez mettre à niveau ASA et FXOS séparément, car ils sont répertoriés séparément dans la liste du répertoire FXOS. L'ensemble ASA comprend toujours ASDM.
- Firepower 2100 en mode plateforme : les images ASA, ASDM et FXOS sont regroupées en un seul ensemble. Les mises à jour de paquets sont gérées par FXOS; vous ne pouvez pas mettre à niveau l'ASA dans le système d'exploitation de l'ASA, donc n'utilisez pas cette procédure pour l'image de l'ASA. Vous *ne pouvez pas* mettre à niveau ASA et FXOS séparément; ils sont toujours regroupés.
- Firepower 1000, 2100 en mode d'appareil, Secure Firewall 3100 : les images ASA, ASDM et FXOS sont regroupées en un seul paquet. Les mises à jour de paquets sont gérées par l'ASA à l'aide de cette procédure. Bien que ces plateformes utilisent l'ASA pour identifier l'image à démarrer, le mécanisme sous-jacent est différent de celui des ASA existants. Consultez la description de la commande ci-dessous pour plus d'informations.
- ASDM pour les modèles : ASDM peut être mis à niveau à partir du système d'exploitation de l'ASA, de sorte que vous n'avez pas besoin d'utiliser uniquement l'image ASDM fournie. Pour Firepower 2100 en mode plateforme et Firepower 4100/9300, les images ASDM que vous téléchargez manuellement ne s'affichent pas dans la liste d'images FXOS; vous devez les gérer à partir de l'ASA.

Remarque Lorsque vous mettez à niveau le paquet de l'ASA, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-782.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.

- ASA virtuel : le paquet de déploiement initial ASA virtuel place l'image de l'ASA dans la partition boot:/ en lecture seule. Lorsque vous mettez à niveau ASA virtuel, vous spécifiez une image différente dans la mémoire flash. Notez que si vous effacez votre configuration ultérieurement avec la commande (**clear configure all**), le ASA virtuel reviendra au chargement de l'image de déploiement d'origine. Le paquet de déploiement initial ASA virtuel comprend également une image ASDM qu'il place dans la mémoire flash. Vous pouvez mettre à niveau l'image ASDM séparément.
- **disk0:** est la mémoire interne. D'autres numéros de lecteur représentent un stockage externe tel qu'un lecteur USB, un SSD ou une carte SD.

Consultez les paramètres par défaut suivants :

- Image ASA :
  - Firepower 1000, 2100 en mode d'appareil,1200/3100/4200 : démarre l'image de démarrage précédente.
  - ISA 3000 : démarre la première image d'application trouvée dans la mémoire flash interne.
  - ASA virtuel : démarre l'image dans la partition boot:/ en lecture seule qui a été créée lors du déploiement initial.
  - Châssis Firepower 4100/9300 : le système FXOS détermine quelle image ASA démarrer. Vous ne pouvez pas utiliser cette procédure pour définir l'image ASA.
  - Firepower 2100 en mode plateforme : le système FXOS détermine quel paquet ASA/FXOS démarrer. Vous ne pouvez pas utiliser cette procédure pour définir l'image ASA.
- Image ASDM sur tous les ASA : démarre la première image ASDM qu'il trouve dans la mémoire flash interne ou, si elle n'en existe pas à cet emplacement, dans la mémoire flash externe.
- Configuration de démarrage : par défaut, l'ASA démarre à partir d'une configuration de démarrage qui est un fichier masqué.

Procédure

Étape 1 Définissez l'emplacement de l'image de démarrage de l'ASA :

*URL***du système de démarrage**

Exemple :

```
ciscoasa(config)# boot system disk0:/images/asa921.bin
```

L'URL peut être :

- **disk** *n***:/**[*path*/]*filename*
- **tftp:**//[*utilisateur*[**:***mot de passe*]**@**]*serveur*[**:***port*]/[*chemin*/]*nom de fichier*

  L'option TFTP n'est pas prise en charge sur tous les modèles.

Firepower 1000, 2100 en mode l'appareil, Secure : vous ne pouvez saisir qu'une seule commande **boot system**. Si vous mettez à niveau vers une nouvelle image, vous devez saisir **no boot system** pour supprimer l'image que vous avez définie. Notez que vous ne pouvez pas avoir une commande **boot system** dans votre configuration; par exemple, si vous avez installé l'image de ROMMON, avez un nouveau périphérique ou avez supprimé la commande manuellement. La commande **boot system** exécute une action lorsque vous la saisissez : le système valide et décompresse l'image et la copie dans l'emplacement de démarrage (un emplacement interne sur disk0 géré par FXOS). La nouvelle image sera chargée lorsque vous rechargerez l'ASA. Si vous changez d'avis avant de téléverser, vous pouvez entrer la commande **no boot system** pour supprimer la nouvelle image de l'emplacement de démarrage, de sorte que l'image actuelle continue de s'exécuter. Vous pouvez même supprimer le fichier image original de la mémoire flash de l'ASA après avoir entré cette commande, et l'ASA démarrera correctement à partir de l'emplacement de démarrage; cependant, nous recommandons de conserver toutes les images que vous souhaitez utiliser dans la mémoire flash, car la commande **boot system** ne fonctionne qu'avec les images dans cette dernière. Contrairement à d'autres modèles, cette commande dans la configuration de démarrage n'affecte pas l'image de démarrage et est essentiellement cosmétique. La dernière image de démarrage chargée sera toujours exécutée lors du rechargement. Si vous n'enregistrez pas la configuration après avoir saisi cette commande, l'ancienne commande sera présente dans votre configuration lors du rechargement, même si la nouvelle image a été démarrée. Assurez-vous d'enregistrer la configuration pour qu'elle reste synchronisée. Vous pouvez uniquement téléverser des images avec le nom de fichier d'origine à partir du site de téléchargement de Cisco. Si vous modifiez le nom de fichier, il ne se téléversera pas. Vous pouvez également recréer l'image de Firewall Threat Defense en chargeant l'image Firewall Threat Defense. Dans ce cas, vous êtes invité à téléverser immédiatement.

autres modèles : vous pouvez entrer jusqu'à quatre entrées de commande de **démarrage système** pour définir différentes images de démarrage dans l'ordre; l'ASA démarre la première image qu'il trouve avec succès. Lorsque vous saisissez la commande **boot system** (démarrage système), elle ajoute une entrée au bas de la liste. Pour réorganiser les entrées de démarrage, vous devez supprimer toutes les entrées à l'aide de la commande **clear configure boot system** et les saisir à nouveau dans l'ordre souhaité. Une seule commande **boot system tftp** peut être configurée et elle doit être la première à être configurée.

Remarque
Si l'ASA est bloqué dans un cycle de démarrage constant, vous pouvez le redémarrer en mode ROMMON. Pour plus d'informations sur le mode ROMMON, consultez Afficher les messages de débogage, à la page 1395.

Exemple :

```
asa(config)# boot system disk0:/cisco-asa-fp2k.9.13.2.SPA
The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.13.2 will do the following:
   - upgrade to the new platform version 2.7.2
   - upgrade to the CSP ASA version 9.13.2
```

```
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
asa(config)#
```

Étape 2 Définissez l'image ASDM pour démarrer :

asdm image disk*n***:/**[*path*/]*filename*

Exemple :

```
ciscoasa(config)# asdm image disk0:/images/asdm721.bin
```

Si vous ne spécifiez pas l'image au démarrage, même si une seule image est installée, l'ASA insère la commande **asdm image** dans la configuration en cours. Pour éviter des problèmes avec la mise à jour automatique (si elle est configurée) et pour éviter la recherche d'image à chaque démarrage, vous devez préciser l'image ASDM que vous souhaitez démarrer dans la configuration de démarrage.

Étape 3 (Facultatif) Définir la configuration de démarrage de sorte qu'elle utilise un fichier connu au lieu du fichier masqué :

boot config disk*n***:/**[*path*/]*filename*

Cette fonctionnalité est importante lorsque vous travaillez avec des configurations volumineuses qui ne tiennent pas dans le répertoire masqué. Si vous enregistrez une grande configuration et que vous voyez le message d'erreur suivant, veillez à enregistrer la configuration dans un nouveau fichier à l'aide de la commande suivante :

```
%Erreur d'écriture. nvRAM:/startup-config (pas d'espace gauche sur le périphérique :)
```

Exemple :

```
ciscoasa(config)# boot config disk0:/configs/startup1.cfg
```

Sauvegarde et restauration de configurations ou d'autres fichiers

Nous vous recommandons de faire des sauvegardes régulières de votre configuration et d'autres fichiers système pour éviter les défaillances du système.

Effectuer une sauvegarde ou une restauration complète du système

Ces procédures décrivent comment sauvegarder et restaurer les configurations et les images dans un fichier tar.gz et le transférer sur votre ordinateur local.

Avant d'entreprendre la sauvegarde ou la restauration

- Vous devez avoir au moins 300 Mo d'espace disque disponible à l'emplacement de sauvegarde ou de restauration avant de lancer une sauvegarde ou une restauration.
- Si vous apportez des modifications à la configuration pendant ou après une sauvegarde, ces modifications ne seront pas incluses dans la sauvegarde. Si vous modifiez une configuration après avoir effectué la sauvegarde, puis effectuez une restauration, cette modification de configuration sera remplacée. Par conséquent, l'ASA pourrait se comporter différemment.
- Vous ne pouvez lancer qu'une seule sauvegarde ou restauration à la fois.
- Vous pouvez uniquement restaurer une configuration sur la même version ASA que celle lorsque vous avez effectué la sauvegarde d'origine. Vous ne pouvez pas utiliser l'outil de restauration pour migrer une configuration d'une version ASA vers une autre. Si une migration de configuration est requise, l'ASA met automatiquement à niveau la configuration de démarrage résidente lorsqu'il charge le nouveau système d'exploitation de l'ASA.
- Si vous utilisez la mise en grappe, vous pouvez uniquement sauvegarder ou restaurer les certificats de configuration de démarrage, de configuration d'exécution et d'identité. Vous devez créer et restaurer une sauvegarde séparément pour chaque unité.
- Si vous utilisez le basculement, vous devez créer et restaurer une sauvegarde séparément pour les unités actives et de secours.
- Si vous définissez une phrase secrète principale pour l'ASA, vous avez besoin de cette phrase secrète principale pour restaurer la configuration de sauvegarde que vous créez avec cette procédure. Si vous ne connaissez pas la phrase secrète principale pour l'ASA, consultez Configurer la phrase secrète principale, à la page 840 pour savoir comment la réinitialiser avant de poursuivre la sauvegarde.
- Si vous importez des données PKCS12 (avec la commande **crypto ca trustpoint**) et que le point de confiance utilise des clés RSA, la paire de clés importée se voit attribuer le même nom que le point de confiance. En raison de cette limite, si vous spécifiez un nom différent pour le point de confiance et sa paire de clés après avoir restauré une configuration ASDM, la configuration de démarrage sera la même que la configuration d'origine, mais la configuration d'exécution comprendra un nom de paire de clés différent. Cela signifie que si vous utilisez des noms différents pour la paire de clés et le point de confiance, vous ne pouvez pas restaurer la configuration d'origine. Pour contourner ce problème, assurez-vous d'utiliser le même nom pour le point de confiance et sa paire de clés.
- Vous ne pouvez pas sauvegarder à l'aide de l'interface de ligne de commande et restaurer à l'aide d'ASDM, ou inversement.
- Chaque fichier de sauvegarde comprend le contenu suivant :
  - Configuration d'exécution
  - Configuration du démarrage
  - Toutes les images de sécurité

    Images de Cisco Secure Desktop et de l'analyse de l'hôte

    Paramètres de Cisco Secure Desktop et de l'analyse de l'hôte

    Images et profils (SVC) d'Secure Client (services client sécurisés)

    Personnalisations et transformations (SVC) d'Secure Client (services client sécurisés)

- Certificats d'identité (inclut les paires de clés RSA liées aux certificats d'identité; exclut les clés autonomes)
- Clés prépartagées VPN
- Configurations SSL VPN
- Cadre personnalisé du profil d'application (APCF)
- Signets
- Personnalisations
- Politique d'accès dynamique (DAP)
- Modules d'extension
- Scripts de préremplissage pour les profils de connexion
- Configuration automatique du serveur mandataire
- Table de traduction
- Web content
- Information de version

Sauvegarder le système

Cette procédure décrit comment effectuer une sauvegarde complète du système.

Procédure

Étape 1 Sauvegardez le système :

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

Exemple :

```
ciscoasa# backup location disk0:/sample-backup]
Backup location [disk0:/sample-backup]?
```

Si vous ne spécifiez pas de **nom** *d'interface*, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

En mode de contexte multiple à partir de l'espace d'exécution du système, saisissez le mot clé **context** pour sauvegarder le contexte spécifié. Chaque contexte doit être sauvegardé individuellement; c'est-à-dire que vous devez saisir à nouveau la commande **backup** pour chaque fichier.

Lors de la sauvegarde des certificats VPN et des clés prépartagées, une clé secrète identifiée par le mot clé **passphrase** est requise pour encoder les certificats. Vous devez fournir une phrase secrète à utiliser pour l'encodage et le décodage des certificats au format PKCS12. La sauvegarde comprend uniquement les paires de clés RSA liées aux certificats et exclut tout certificat autonome.

L'**emplacement** de sauvegarde peut être un disque local ou une URL distante. Si vous ne fournissez pas d'emplacement, les noms par défaut suivants sont utilisés :

- Mode unique—disk0 :*hostname*.backup.*timestamp*.tar.gz
- Mode multiple—disk0 :*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

Étape 2 Suivez les instructions :

Exemple :

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco.
You will be required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file
is used to restore to a device with a different master passphrase,
you will need to provide the current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

Restaurer la sauvegarde

Vous pouvez spécifier les configurations et les images à restaurer à partir d'un fichier zip tar.gz sur votre ordinateur local.

Procédure

Étape 1 Restaurez le système à partir du fichier de sauvegarde.

restore [**/noconfirm**] [**context** *ctx-name*] [**passphrase** *value*] [**location** *path*]

Exemple :

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
```

```
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
```

Lorsque vous utilisez le mot clé **context** pour restaurer plusieurs contextes, chaque fichier de contexte sauvegardé doit être restauré individuellement; c'est-à-dire que vous devez saisir à nouveau la commande **restore** pour chaque fichier.

Étape 2 Suivez les instructions :

Exemple :

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version,
some configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption.
Master passphrase is required to restore running configuration,
startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to
this device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside,
the IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside,
the IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations.
Do not overwrite configuration file if you want to preserve the old http-
and https-proxy configurations.

Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates.
The default is cisco. If the passphrase is not correct, certificates will not be restored.
```

```
No passphrase was provided for identity certificates.
Using the default value: cisco. If the passphrase is not correct,
certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

Configurer la sauvegarde et la restauration automatiques (ISA 3000)

Sur l'ISA 3000, vous pouvez configurer des sauvegardes automatiques vers un emplacement particulier chaque fois que vous enregistrez votre configuration à l'aide de **write memory**.

La restauration automatique vous permet de configurer facilement de nouveaux périphériques avec une configuration complète chargée sur une carte de mémoire flash SD. La restauration automatique est activée dans la configuration d'usine par défaut.

Configurer la sauvegarde automatique (ISA 3000)

Sur l'ISA 3000, vous pouvez configurer des sauvegardes automatiques vers un emplacement particulier chaque fois que vous enregistrez votre configuration à l'aide de **write memory**.

Avant de commencer

Cette fonctionnalité est uniquement disponible sur l'ISA 3000.

Procédure

Étape 1 Définissez les paramètres du paquet de sauvegarde :

backup-package backup [**interface** *name*] **location** {**disk***n***:** | *url*} [**passphrase** *string*]

- **interface** *name* : spécifie l'interface permettant d'atteindre l'URL de sauvegarde, si vous spécifiez un stockage hors périphérique. Si vous ne spécifiez pas de nom d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.
- **location** {**disk***n***:** | *url*} : spécifie le support de stockage à utiliser pour la sauvegarde des données. Vous pouvez définir une URL ou un stockage local : disk0 est le lecteur flash interne, disk1 est une clé de mémoire USB facultative sur USB 1, disk2 est une clé de mémoire USB facultative sur USB 2. Et disk3 est la carte mémoire SD. Notez que les paramètres par défaut pour la restauration automatique utilisent disk3.
- **passphrase** *string* : définit la phrase secrète pour sécuriser les données sauvegardées. Notez que les paramètres par défaut pour la restauration automatique utilisent « cisco » comme phrase secrète.

Ces paramètres sont également utilisés par défaut avec la commande manuelle **backup**. Consultez Sauvegarder le système, à la page 1355. Notez que si vous utilisez la commande manuelle **backup** lorsque la sauvegarde ou

la restauration automatiques sont activées, le système enregistre un fichier de sauvegarde avec le nom spécifié, ainsi que le nom « auto-backup-asa.tgz » utilisé par la sauvegarde et la restauration automatiques.

Exemple :

```
ciscoasa(config)# backup-package backup location disk3: passphrase cisco
```

Étape 2 Activez le mode automatique pour la sauvegarde et la restauration :

backup-package backup auto

Lorsque vous enregistrez la configuration à l'aide de **write memory**, la configuration est automatiquement enregistrée à l'emplacement de sauvegarde ainsi que dans la configuration de démarrage. Le fichier de sauvegarde est intitulé « auto-backup-asa.tgz ». Pour désactiver les sauvegardes automatiques, utilisez la forme **no** de la commande.

Exemple :

```
ciscoasa(config)# backup-package backup auto
```

Configurer la restauration automatique (ISA 3000)

Le mode de restauration automatique restaure la configuration système sur un périphérique sans intervention de l'utilisateur. Par exemple, vous insérez une carte de mémoire SD contenant une configuration de sauvegarde enregistrée dans un nouveau périphérique, puis mettez celui-ci sous tension. Lorsque le périphérique se manifeste, il vérifie la carte SD pour décider si la configuration système doit être restaurée. (La restauration n'est lancée que si le fichier de sauvegarde comporte l'« empreinte digitale » d'un autre périphérique. L'empreinte du fichier de sauvegarde est mise à jour pour correspondre au périphérique actuel lors d'une opération de sauvegarde ou de restauration. Donc, si le périphérique a déjà effectué une restauration ou s'il a créé sa propre sauvegarde, la restauration automatique est ignorée.) Si l'empreinte indique qu'une restauration est requise, le périphérique remplace la configuration système (startup-config, running-config, configuration du SSL VPN, etc.; consultez Sauvegarder le système, à la page 1355 pour plus de détails sur le contenu de la sauvegarde). Lorsque le périphérique a terminé son démarrage, il exécute la configuration enregistrée.

La restauration automatique est activée dans la configuration d'usine par défaut. Vous pouvez donc facilement configurer de nouveaux périphériques avec une configuration complète chargée sur une carte de mémoire SD sans avoir à effectuer de préconfiguration du périphérique.

Étant donné que le périphérique doit décider dès le début du processus de démarrage si la configuration système doit être restaurée, il vérifie les variables ROMMON pour déterminer si le périphérique est en mode de restauration automatique et pour obtenir l'emplacement de la configuration de sauvegarde. Les variables ROMMON suivantes sont utilisées :

- **RESTORE_MODE =** {**auto** | **manual**}

  La valeur par défaut est **auto**.

- **RESTORE_LOCATION =** {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  La valeur par défaut est **disk3:**.

- **RESTORE_PASSPHRASE** = *key*

  La valeur par défaut est **cisco**.

Pour modifier les paramètres de restauration automatique, procédez comme suit.

Avant de commencer

- Cette fonctionnalité est uniquement disponible sur l'ISA 3000.
- Si vous utilisez les paramètres de restauration par défaut, une carte de mémoire SD doit être installée (numéro de pièce SD-IE-1GB=).
- Si vous devez restaurer la configuration par défaut pour vous assurer que la restauration automatique est activée, utilisez la commande **configure factory default**. Cette commande est uniquement disponible en mode de pare-feu transparent. Par conséquent, si vous êtes en mode de pare-feu routé, utilisez d'abord la commande **firewall transparent**.

Procédure

Étape 1 Définissez les paramètres du paquet de restauration.

backup-package restore location {**disk***n***:** | *url*} [**passphrase** *string*]

- **location disk***n***:** : spécifie le support de stockage à utiliser pour la restauration des données. disk0 est le lecteur flash interne, disk1 est une clé de mémoire USB facultative sur USB 1 et disk2 est une clé de mémoire USB facultative sur USB 2. Et disk3 est la carte mémoire SD. La valeur par défaut est disk3.
- **passphrase** *string* : définit la phrase secrète pour lire les données sauvegardées. La valeur par défaut est « cisco ».

Ces paramètres sont également utilisés par défaut avec la commande manuelle **restore**. Consultez Sauvegarder le système, à la page 1355.

Exemple :

```
ciscoasa(config)# backup-package restore location disk1: passphrase $upe3rnatural
```

Étape 2 Activez ou désactivez le mode automatique pour la restauration.

[**no**]**backup-package restore auto**

Le nom du fichier restauré est « auto-backup-asa.tgz ».

Exemple :

```
ciscoasa(config)# no backup-package restore auto
```

Sauvegarder la configuration en mode unique ou la configuration système en mode multiple

En mode de contexte unique ou à partir de la configuration système en mode multiple, vous pouvez copier la configuration de démarrage ou la configuration en cours d'exécution sur un serveur externe ou dans la mémoire flash locale.

Avant de commencer

(Facultatif) Spécifiez l'interface par laquelle l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

Procédure

Sauvegardez la configuration en utilisant l'un des types de serveur suivants :

- Copiez sur un serveur TFTP :

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **tftp:**//*server*[/*path*]/*dst_filename*

  Exemple :

  ```
  ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg
  ```

- Copiez sur un serveur FTP :

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **ftp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  Exemple :

  ```
  ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg
  ```

- Copiez sur un serveur SMB :

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **smb:**//[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  Exemple :

  ```
  ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg
  ```

- Copiez sur un serveur SCP :

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **scp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*[**;int=***interface_name*]

  Exemple :

  ```
  ciscoasa# copy startup-config
  ```

```
scp://pilot:moya@10.86.94.170/new-startup.cfg
```

L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur SCP.

- Copiez dans la mémoire flash locale :

  copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  Exemple :

```
ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg
```

  Assurez-vous que le répertoire de destination existe. S'il n'existe pas, créez d'abord le répertoire à l'aide de la commande **mkdir**.

Sauvegarder une configuration de contexte ou un autre fichier dans la mémoire flash

Copiez les configurations de contexte ou les autres fichiers qui se trouvent sur la mémoire flash locale en saisissant l'une des commandes suivantes dans l'espace d'exécution du système.

Avant de commencer

(Facultatif) Spécifiez l'interface par laquelle l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

Procédure

Sauvegardez une configuration de contexte en utilisant l'un des types de serveur suivants :

- Copiez depuis la mémoire flash vers un serveur TFTP :

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **tftp://***server*[*/path*]*/dst_filename*

  Exemple :

```
ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin
```

- Copiez depuis la mémoire flash vers un serveur FTP :

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  Exemple :

```
ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin
```

- Copiez depuis la mémoire flash vers un serveur SMB :

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  Exemple :

```
ciscoasa# copy /noconfirm copy disk0:/asdm.bin
smb://chiana:dargo@10.1.1.67/asdm.bin
```

- Copiez depuis la mémoire flash vers un serveur SCP :

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  Exemple :

```
ciscoasa# copy disk0:/context1.cfg
scp://pilot:moya@10.86.94.170/context1.cfg
```

  L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur SCP.

- Copiez depuis la mémoire flash vers la mémoire flash locale :

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  Exemple :

```
ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg
```

  Assurez-vous que le répertoire de destination existe. S'il n'existe pas, créez d'abord le répertoire à l'aide de la commande **mkdir**.

Sauvegarder une configuration de contexte dans un contexte

En mode de contexte multiple, à partir d'un contexte, vous pouvez effectuer les sauvegardes suivantes.

Procédure

Étape 1 Copiez la configuration en cours d'exécution à l'emplacement de la configuration de démarrage (si, sur un serveur distant, elle est connectée au contexte d'administration). L'emplacement de la configuration de démarrage est spécifié par la commande **config-url**.

copy running-config startup-config

Exemple :

```
ciscoasa/contexta# copy running-config startup-config
```

Étape 2 Copiez la configuration en cours d'exécution sur un serveur FTP ou TFTP connecté au réseau *contextuel*.

copy running-config {**ftp** | **tftp**}**:**//*url*/*dest_filename*

Consultez l'aide de la commande **copy** pour connaître les options d'URL exactes.

Si vous activez le stockage privé (**storage-url private**), d'autres options de serveur sont disponibles. Cependant, SCP n'est pas pris en charge dans un contexte utilisant la pile CiscoSSH.

Exemple :

```
ciscoasa/contexta# copy running-config tftp:/10.89.6.8/configs/1010-1.cfg
```

Copier la configuration à partir de l'affichage du terminal

Procédure

Étape 1 Imprimez la configuration sur le terminal :

more system:running-config

Étape 2 Copiez le résultat de cette commande, puis collez la configuration dans un fichier texte.

Sauvegarder les fichiers supplémentaires à l'aide des commandes d'exportation et d'importation

Les fichiers supplémentaires essentiels à votre configuration peuvent inclure les éléments suivants :

- Les fichiers que vous importez à l'aide de la commande **import webvpn**. Actuellement, ces fichiers comprennent les personnalisations, les listes d'URL, le contenu Web, les modules d'extension et les traductions de langue.
- Politiques DAP (dap.xml).
- Configurations CSD (data.xml).
- Clés et certificats numériques.
- Base de données des utilisateurs CA locale et fichiers d'état des certificats.

L'interface de ligne de commande vous permet de sauvegarder et de restaurer des éléments individuels de votre configuration à l'aide des commandes **export** et **import**.

Pour sauvegarder ces fichiers, par exemple, les fichiers que vous avez importés avec la commande **import webvpn** ou les certificats, procédez comme suit.

Procédure

Étape 1 Exécutez la ou les commandes **show** applicables comme suit :

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

Étape 2 Exécutez la commande **export** pour le fichier que vous souhaitez sauvegarder (dans cet exemple, le fichier rdp) :

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

Utiliser un script pour sauvegarder et restaurer des fichiers

Vous pouvez utiliser un script pour sauvegarder et restaurer les fichiers de configuration de votre ASA, y compris toutes les extensions que vous importez via l'interface de ligne de commande **import webvpn**, les fichiers XML de configuration CSD et le fichier XML de configuration DAP. Pour des raisons de sécurité, nous vous déconseillons d'effectuer des sauvegardes automatisées des clés et des certificats numériques ou de la clé CA locale.

Cette section fournit des instructions à cet effet et comprend un exemple de script que vous pouvez utiliser tel quel ou modifier en fonction de votre environnement. L'exemple de script est propre à un système Linux. Pour l'utiliser sur un système Microsoft Windows, vous devez le modifier en utilisant la logique de l'exemple.

Remarque Vous pouvez également utiliser les commandes **backup** et **restore**. Consultez Effectuer une sauvegarde ou une restauration complète du système, à la page 1353 pour de plus amples renseignements.

Avant d'utiliser des scripts de sauvegarde et de restauration

Si vous souhaitez utiliser un script pour sauvegarder et restaurer une configuration ASA, effectuez d'abord les tâches suivantes :

- Installez Perl avec un module Expect.
- Installez un client SSH qui peut atteindre l'ASA.
- Installez un serveur TFTP pour envoyer des fichiers de l'ASA vers le site de sauvegarde.

Une autre option consiste à utiliser un outil disponible dans le commerce. Vous pouvez placer la logique de ce script dans un tel outil.

Exécuter le script

Pour exécuter un script de sauvegarde et de restauration, procédez comme suit.

Procédure

Étape 1 Téléchargez ou copiez et collez le fichier de script à n'importe quel emplacement de votre système.

Étape 2 Dans la ligne de commande, saisissez **Perl***scriptname*, où *scriptname* est le nom du fichier de script.

Étape 3 Appuyez sur **Entrée**.

Étape 4 Le système vous invite à saisir des valeurs pour chaque option. Vous pouvez également saisir des valeurs pour les options lorsque vous saisissez la commande **Perl***scriptname* avant d'appuyer sur **Enter** (Entrée). Dans tous les cas, le script exige que vous saisissiez une valeur pour chaque option.

Étape 5 Le script commence à s'exécuter et affiche les commandes qu'il émet, ce qui vous fournit un enregistrement des interfaces de ligne de commande. Vous pouvez utiliser ces interfaces de ligne de commande pour une restauration ultérieure, ce qui est particulièrement utile si vous ne souhaitez restaurer qu'un ou deux fichiers.

Exemple de script

```
#!/usr/bin/perl
#Description: The objective of this script is to show how to back up
configurations/extensions.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#       -r: Restore with an argument that specifies the file name. This file is produced
during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F`;
chop($date);
my $exp = new Expect();
```

```
getopts("h:u:p:w:e:s:r:",\%options);
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("$enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
```

```
  print "$cli\n";
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}


sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub url_list {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn url-list\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
     $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
```

```
      $obj->send("$cli\n");
      $obj->expect(15, "$prompt#" );
   }
}

sub dap {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir dap.xml\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub csd {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir sdesktop\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub webcontent {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn webcontent\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /No custom/;
     next unless (/^.+\s+.+$/);
     ($url, $type) = split(/\s+/,$_);
     $turl = $url;
     $turl =~ s/\/\+//;
     $turl =~ s/\+\//-/;
     $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
```

```
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}

sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
      $storage = "tftp://$tstr";
  }
  else {
      print "Enter TFTP host name or IP address:";
      chop($tstr=<>);
      $storage = "tftp://$tstr";
  }
  if (defined($options{h})) {
      $asa = $options{h};
  }
  else {
      print "Enter ASA host name or IP address:";
      chop($asa=<>);
  }

  if (defined ($options{u})) {
      $user= $options{u};
  }
  else {
      print "Enter user name:";
      chop($user=<>);
  }
```

```
  if (defined ($options{w})) {
      $password= $options{w};
  }
  else {
      print "Enter password:";
      chop($password=<>);
  }
  if (defined ($options{p})) {
      $prompt= $options{p};
  }
  else {
      print "Enter ASA prompt:";
      chop($prompt=<>);
  }
  if (defined ($options{e})) {
      $enable = $options{e};
  }
  else {
      print "Enter enable password:";
      chop($enable=<>);
  }

  if (defined ($options{r})) {
     $restore = 1;
     $restore_file = $options{r};
  }
}
```

Échange à chaud d'un SSD sur Cisco Secure Firewall

Si vous avez deux disques SSD, ils forment un RAID lorsque vous démarrez. Vous pouvez effectuer les tâches suivantes au niveau de l'interface de ligne de commande lorsque le pare-feu est sous tension :

- Échangez à chaud un des disques SSD : si un disque SSD est défectueux, vous pouvez le remplacer. Notez que si vous n'avez qu'un seul disque SSD, vous ne pouvez pas le retirer tant que le pare-feu est sous tension.
- Retirez un des disques SSD : si vous avez deux disques SSD, vous pouvez en retirer un.
- Ajouter un deuxième SSD : si vous avez un deuxième SSD, vous pouvez en ajouter un deuxième et former un RAID.

⚠

Mise en garde Ne retirez pas physiquement un SSD sans l'avoir supprimé du RAID en suivant cette procédure. Vous pourriez entraîner des pertes de données.

Procédure

Étape 1 Retirez l'un des disques SSD.

a) Retirez le SSD du RAID.

raid remove-secure local-disk {**1** | **2**}

Le mot clé **remove-secure** supprime le SSD du RAID, désactive la fonction de disque à chiffrement automatique et effectue un effacement sécurisé du SSD. Si vous souhaitez uniquement retirer le SSD du RAID et conserver les données intègres, vous pouvez utiliser le mot clé **remove**.

Exemple :

```
ciscoasa(config)# raid remove-secure local-disk 2
```

b) Surveiller l'état RAID jusqu'à ce que SSD ne s'affiche plus dans l'inventaire.

show raid

Une fois le SSD retiré du RAID, l'**exploitabilité** et **l'état du lecteur** s'affichent comme **dégradés**. Le deuxième lecteur ne sera plus répertorié en tant que disque membre.

Exemple :

```
ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
```

```
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) Retirez physiquement le disque SSD du châssis.

Étape 2 Ajouter un disque SSD.

a) Ajoutez physiquement le SSD dans le logement vide.

b) Ajoutez le SSD au RAID.

raid add local-disk {**1** | **2**}

La synchronisation du nouveau SSD avec le RAID peut prendre plusieurs heures, pendant laquelle le pare-feu est complètement opérationnel. Vous pouvez même redémarrer et la synchronisation se poursuivra après la mise sous tension. Utilisez la commande **show raid** pour afficher l'état.

Si vous installez un disque SSD qui a été utilisé précédemment sur un autre système et qui est toujours verrouillé, saisissez la commande suivante :

raid add local-disk {**1** | **2**} *psid*

Le *psid* est imprimé sur l'étiquette fixée à l'arrière du disque SSD. Sinon, vous pouvez redémarrer le système et le SSD sera formaté et ajouté au RAID.

Historique des logiciels et des configurations

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Client et serveur Secure Copy	9.1(5)/9.2(1)	L'ASA prend désormais en charge le client et le serveur Secure Copy (SCP) pour transférer des fichiers vers et depuis un serveur SCP. Nous avons introduit les commandes suivantes : **ssh pubkey-chain**, **server (ssh pubkey-chain)**, **key-string**, **key-hash**, **ssh stricthostkeycheck**. Nous avons modifié la commande suivante : **copy scp**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Chiffrement SSH et d'intégrité configurables	9.1(7)9.4(3)9.5(3)9.6(1)	Les utilisateurs peuvent sélectionner des modes de chiffrement lors de la gestion du chiffrement SSH et peuvent configurer le HMAC et le chiffrement pour divers algorithmes d'échange de clés. Vous souhaiterez peut-être modifier les chiffres pour qu'ils soient plus ou moins stricts, selon votre application. Notez que la performance de la copie sécurisée dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier les chiffres proposés, utilisez **ssh cipher encryption custom aes128-cbc**, par exemple. Nous avons introduit les commandes suivantes : **ssh cipher encryption**, **ssh cipher integrity**
Vérification du certificat du serveur de mise à jour automatique activée par défaut	9.2(1)	La vérification du certificat du serveur de mise à jour automatique est maintenant activée par défaut; pour les nouvelles configurations, vous devez explicitement désactiver la vérification de certificat. Si vous effectuez une mise à niveau à partir d'une version antérieure et que vous n'avez pas activé la vérification de certificat, la vérification de certificat n'est pas activée, et l'avertissement suivant s'affiche : `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` La configuration sera migrée vers la configuration explicite sans vérification. **auto-update server no-verification** Nous avons modifié la commande suivante : **auto-update server** {**verify-certificate** | **no-verification**}.
Sauvegarde et restauration du système à l'aide de l'interface de ligne de commande	9.3(2)	Vous pouvez maintenant sauvegarder et restaurer des configurations système complètes, y compris les images et les certificats, à l'aide de l'interface de ligne de commande. Nous avons introduit les commandes suivantes : **backup** et **restore**.
Récupération et chargement d'une nouvelle image ASA 5506W-X	9.4(1)	Nous prenons désormais en charge la récupération et le chargement d'une nouvelle image ASA 5506W-X. Nous avons introduit la commande suivante : **hw-module module wlan recover image**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Sauvegarde et restauration automatiques pour l'ISA 3000	9.7(1)	Vous pouvez activer la fonction de sauvegarde automatique et/ou de restauration automatique en utilisant les paramètres prédéfinis dans les commandes de sauvegarde et de restauration. Les scénarios de ces fonctionnalités comprennent la configuration initiale à partir d'un support externe; le remplacement de l'appareil; la restauration à un état opérationnel. Nous avons introduit les commandes suivantes : **backup-package location, backup-package auto, show backup-package status, show backup-package summary**
La pile CiscoSSH requiert un accès SSH lors de l'utilisation du client SCP	9.17(1)	Si vous utilisez la pile CiscoSSH, ou utilisez la commande ASA **copy** de l'ASA pour copier un fichier vers ou à partir d'un serveur SCP, vous devez activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP à l'aide de la commande **ssh**.
Prise en charge RAID pour les SSD sur le pare-feu Secure Firewall 3100	9.17(1)	Les disques SSD sont des disques à chiffrement automatique (SED), et si vous avez deux disques SSD, ils forment un RAID logiciel. Commandes nouvelles ou modifiées : **raid, show raid, show ssd**



CHAPITRE 45

Automatisation de la réponse pour les événements système

Ce chapitre décrit comment configurer le gestionnaire d'événements intégré (EEG)

- À propos de l'EEG, à la page 1377
- Lignes directrices pour l'EEG, à la page 1379
- Configurer l'EEG, à la page 1379
- Exemples d'EEG, à la page 1387
- Supervision de l'EEG, à la page 1388
- Historique de l'EEG, à la page 1388

À propos de l'EEG

Le service EEG vous permet de déboguer les problèmes et fournit une journalisation à usage général pour le dépannage. Il y a deux composants : les événements auxquels l'EEG répond ou écoute, et les applets de gestionnaire d'événements qui définissent les actions ainsi que les événements auxquels l'EEG répond. Vous pouvez configurer plusieurs applets de gestionnaire d'événements pour répondre à différents événements et effectuer des actions différentes.

Événements pris en charge

L'EEG prend en charge les événements suivants :

- Journal système : l'ASA utilise les ID des messages de journal système pour identifier les messages de journal système qui déclenchent un applet de gestionnaire d'événements. Vous pouvez configurer plusieurs événements de journal système, mais les ID des messages de journal système ne peuvent pas se chevaucher dans un seul applet de gestionnaire d'événements.
- Minuteries : vous pouvez utiliser des minuteries pour déclencher des événements. Vous ne pouvez configurer chaque minuterie qu'une seule fois pour chaque applet de gestionnaire d'événements. Chaque applet de gestionnaire d'événements peut avoir jusqu'à trois minuteries. Les trois types de minuteries sont les suivants :
  - Les minuteries de surveillance (périodiques) déclenchent un applet de gestionnaire d'événements après la période spécifiée suivant la fin des actions de l'applet et redémarrent automatiquement.

- Les minuteries de compte à rebours (à usage unique) déclenchent un applet de gestionnaire d'événements une fois après la période spécifiée et ne redémarrent pas à moins d'être supprimées, puis rajoutées.
- Les minuteries absolues (une fois par jour) déclenchent un événement une fois par jour à une heure spécifiée et redémarrent automatiquement. Le format de l'heure du jour hh:mm:ss.

  Vous ne pouvez configurer qu'un seul événement de minuterie de chaque type pour chaque applet de gestionnaire d'événements.

- Aucun : l'événement Aucun est déclenché lorsque vous exécutez un applet de gestionnaire d'événements manuellement à l'aide de l'interface de ligne de commande ou d'ASDM.
- Plantage : l'événement de plantage est déclenché lorsque l'ASA tombe en panne. Dans certains scénarios, un plantage forcé est déclenché :

  Si l'ASA est configuré pour se recharger en cas d'épuisement du bloc et que l'ASA reste à court de mémoire pendant une durée configurée, il envoie le journal système et recueille des données de dépannage. L'ASA force le plantage et déclenche le processus de rechargement pour libérer le bloc de mémoire. Dans une configuration à haute disponibilité, dans de tels cas, le basculement est déclenché. Dans une configuration de grappe, le nœud quitte la grappe.

  Quelle que soit la valeur de la commande **output**, les commandes **action** sont dirigées vers le fichier crashinfo. La sortie est générée avant la commande **show tech**.

Actions sur les applets de gestionnaire d'événements

Lorsqu'un applet de gestionnaire d'événements est déclenché, les actions sur cet applet sont effectuées. Chaque action a un numéro utilisé pour spécifier la séquence des actions. Le numéro de séquence doit être unique dans un applet de gestionnaire d'événements. Vous pouvez configurer plusieurs actions pour un applet de gestionnaire d'événements. Les commandes sont des commandes d'interface de ligne de commande typiques, telles que **show blocks**.

Destinations de sortie

Vous pouvez envoyer le résultat des actions à un emplacement spécifié à l'aide de la commande **output**. Une seule valeur de sortie peut être activée à la fois. La valeur par défaut est **output none**. Cette valeur annule toute sortie des commandes **action**. La commande s'exécute en mode de configuration globale en tant qu'utilisateur ayant le niveau de privilège 15 (le plus élevé). La commande ne peut accepter aucune entrée, car elle est désactivée. Vous pouvez envoyer la sortie des commandes **action** de l'interface de ligne de commande à l'un des trois emplacements suivants :

- **None** (Aucun), qui est la valeur par défaut et ignore la sortie.
- **Console**, qui envoie les données de sortie à la console ASA.
- **File** (Fichier), qui envoie la sortie dans un fichier. Les quatre options de fichiers suivantes sont disponibles :
  - **Create a unique file** (Créer un fichier unique), qui crée un nouveau fichier avec un nom unique chaque fois qu'un applet de gestionnaire d'événements est invoqué.
  - **Create/overwrite a file** (Créer/remplacer un fichier), qui remplace un fichier spécifié chaque fois qu'un applet de gestionnaire d'événements est invoqué.

- **Create/append to a file** (Créer/ajouter à un fichier), qui s'ajoute à un fichier spécifié chaque fois qu'un applet de gestionnaire d'événements est invoqué. Si le fichier n'existe pas encore, il est créé.
- **Create a set of files** (Créer un ensemble de fichiers), ce qui crée un ensemble de fichiers portant des noms uniques qui sont tournés chaque fois qu'un applet de gestionnaire d'événements est invoqué.

Lignes directrices pour l'EEG

Cette section décrit les lignes directrices et les limites que vous devez vérifier avant de configurer l'EEG.

Directives relatives au mode contextuel

Non pris en charge en mode de contexte multiple.

Directives supplémentaires

- Lors d'un plantage, l'état de l'ASA est généralement inconnu. Certaines commandes peuvent ne pas être exécutées en toute sécurité dans cette condition.
- Le nom d'un applet de gestionnaire d'événements ne peut pas contenir d'espaces.
- Vous ne pouvez pas modifier les paramètres des événements None (Aucun) et Cashinfo (Renseignements sur le plantage).
- Les performances peuvent être affectées, car les messages du journal système sont envoyés à l'EEG pour traitement.
- La sortie par défaut est **output none** pour chaque applet de gestionnaire d'événements. Pour modifier ce paramètre, vous devez entrer une valeur de sortie différente.
- Vous ne pouvez avoir qu'une seule option de sortie définie pour chaque applet de gestionnaire d'événements.

Configurer l'EEG

La configuration de l'EEG comprend les tâches suivantes :

Procédure

Étape 1 Créer un applet de gestionnaire d'événements et configurer les événements, à la page 1380.
Étape 2 Configurer une action et des destinations pour la sortie d'une action, à la page 1381.
Étape 3 Exécuter un applet de gestionnaire d'événements, à la page 1383.
Étape 4 Suivre l'allocation de mémoire et l'utilisation de la mémoire, à la page 1384.

Créer un applet de gestionnaire d'événements et configurer les événements

Pour créer un applet de gestionnaire d'événements et configurer les événements, procédez comme suit :

Procédure

Étape 1 Créez un applet de gestionnaire d'événements et passez en mode de configuration de l'applet de gestionnaire d'événements.

event manager applet *nom*

Exemple :

```
ciscoasa(config)# event manager applet exampleapplet1
```

L'argument *name* peut comporter jusqu'à 32 caractères alphanumériques. Les espaces ne sont pas autorisées

Pour supprimer un applet de gestionnaire d'événements, saisissez la forme **no** de cette commande.

Étape 2 Décrivez un applet de gestionnaire d'événements.

description *texte*

Exemple :

```
ciscoasa(config-applet)# description applet1example
```

L'argument *text* peut comporter jusqu'à 256 caractères. Vous pouvez inclure des espaces dans le texte de la description si celui-ci est placé entre guillemets.

Étape 3 Pour configurer un événement donné, saisissez l'une des commandes suivantes. Pour supprimer l'événement configuré, saisissez la forme **no** (non) de chacune des commandes.

- Pour configurer un événement du journal système, identifiez un seul message de journal système ou une plage de messages de journal système qui déclenchent un applet de gestionnaire d'événements.

  event syslog id *nnnnnn* [-*nnnnnn*] [**occurs** *n*] [**period** *seconds*]

  Exemple :

  ```
  ciscoasa(config-applet)# event syslog id 106201
  ```

  L'argument *nnnnnn* identifie l'ID du message de journal système. La paire mot clé-argument **occurs** *n* indique le nombre de fois que le message du journal système doit se produire pour qu'un applet de gestionnaire d'événements soit invoqué. La valeur par défaut est de 1 occurrence toutes les 0 secondes. Les valeurs valides sont comprises entre 1 et 4294967295. La paire mot clé-argument **period** *seconds* indique le nombre de secondes pendant lesquelles l'événement doit se produire et limite la fréquence d'appel d'un applet de gestionnaire d'événements au maximum une fois dans la période configurée. Les valeurs valides sont comprises entre 0 et 604800. La valeur 0 signifie qu'aucune période n'est définie.

- Pour configurer un événement afin qu'il se produise une fois par période configurée et redémarre automatiquement.

  event timer watchdog time *seconds*

Exemple :

```
ciscoasa(config-applet)# event timer watchdog time 30
```

Le nombre de secondes peut aller de 1 à 604800.

- Pour configurer un événement afin qu'il se produise une seule fois et ne redémarre pas à moins qu'il ne soit supprimé, puis rajouté.

  event timer countdown time *seconds*

  Exemple :

  ```
  ciscoasa(config-applet)# event timer countdown time 60
  ```

  Le nombre de secondes peut aller de 1 à 604800. Utilisez la forme **no** de cette commande pour supprimer un événement de minuterie de compte à rebours.

  Remarque
  Cette minuterie se réexécute lorsque vous redémarrez s'il s'agit de la configuration de démarrage.

- Pour configurer un événement afin qu'il se produise une fois par jour à une heure précise et qu'il redémarre automatiquement.

  event timer absolute time *hh:mm:ss*

  Exemple :

  ```
  ciscoasa(config-applet)# event timer absolute time 10:30:20
  ```

  Le format de l'heure du jour hh:mm:ss. La plage horaire va de 00:00:00 (minuit) à 23:59:59.

- Déclenchez un événement de plantage lorsque l'ASA tombe en panne.

  event crashinfo

  Exemple :

  ```
  ciscoasa(config-applet)# event crashinfo
  ```

  Quelle que soit la valeur de la commande **output**, les commandes **action** sont dirigées vers le fichier crashinfo. La sortie est générée avant la commande **show tech**.

Configurer une action et des destinations pour la sortie d'une action

Pour configurer une action et des destinations spécifiques pour l'envoi de la sortie d'une action, procédez comme suit :

Procédure

Étape 1 Configurez une action sur un applet de gestionnaire d'événements.

action *n* **cli command** *"command"*

Exemple :

```
ciscoasa(config-applet)# action 1 cli command "show version"
```

L'option *n* est un ID d'action. Les ID valides vont de 0 à 4294967295. La valeur de l'option *command* doit être entre guillemets, sinon une erreur se produit si la commande comporte plusieurs mots. La commande s'exécute en mode de configuration globale en tant qu'utilisateur ayant le niveau de privilège 15 (le plus élevé). La commande ne peut accepter aucune entrée, car elle est désactivée. Utilisez l'option **noconfirm** si la commande la propose.

Étape 2 Choisissez l'une des options de destination de sortie disponibles. Utilisez la forme **no** dde chaque commande pour supprimer une destination de sortie.

- L'option **None** annule toute sortie des commandes **action**, ce qui correspond au paramètre par défaut :

  output none

  Exemple :

  ```
  ciscoasa(config-applet)# output none
  ```

- L'option **Console** envoie le résultat des commandes **action** à la console.

  output console

  Exemple :

  ```
  ciscoasa(config-applet)# output console
  ```

  Remarque
  L'exécution de cette commande affecte les performances.

- L'option **New File** envoie la sortie des commandes **action** vers un nouveau fichier pour chaque applet de gestionnaire d'événements invoqué.

  output file new

  Exemple :

  ```
  ciscoasa(config-applet)# output file new
  ```

  Le nom de fichier a le format eem-*Applet-horodatage.log*, dans lequel *Applet* est le nom de l'Applet du gestionnaire d'événements et *Horodatage* est un horodatage datant au format YYYMMMDD-hhmmss.

- L'option **New Set of Rotated Files** crée un ensemble de fichiers qui sont tournés. Lorsqu'un nouveau fichier doit être écrit, le fichier le plus ancien est supprimé et tous les fichiers suivants sont renumérotés avant l'écriture du premier fichier.

  output file rotate *n*

  Exemple :

  ```
  ciscoasa(config-applet)# output file rotate 50
  ```

  Le fichier le plus récent est indiqué par 0, et le fichier le plus ancien est indiqué par le nombre le plus élevé (*n*-1). L'option *n* est la valeur de rotation. Les valeurs valides sont comprises entre 2 et 100. Le format du nom de fichier est eem-*Applet*-*x*.log, dans lequel *Applet* est le nom de l'applet et *x* est le numéro de fichier.

- L'option **Single Overwritten File** écrit la sortie de la commande **action** dans un fichier unique, qui est remplacé chaque fois.

  output file overwrite *filename*

  Exemple :

  ```
  ciscoasa(config-applet)# output file overwrite examplefile1
  ```

  L'argument *filename* est un nom de fichier local (pour l'ASA). Cette commande peut également utiliser des fichiers ciblés FTP, TFTP et SMB.

- L'option **Single Appended File** écrit la sortie de la commande **action** dans un fichier unique, mais ce fichier est ajouté à chaque fois.

  output file append *filename*

  Exemple :

  ```
  ciscoasa(config-applet)# output file append examplefile1
  ```

  L'argument *filename* est un nom de fichier local (pour l'ASA).

Exécuter un applet de gestionnaire d'événements

Pour exécuter un applet de gestionnaire d'événements, procédez comme suit :

Procédure

Exécutez un applet de gestionnaire d'événements.

event manager run *applet*

Exemple :

```
ciscoasa# event manager run exampleapplet1
```

Si vous exécutez un applet de gestionnaire d'événements qui n'a pas été configuré avec la commande **event none**, une erreur se produit. L'argument *applet* est le nom de l'applet de gestionnaire d'événements.

Suivre l'allocation de mémoire et l'utilisation de la mémoire

Pour consigner l'allocation de mémoire et l'utilisation de la mémoire, procédez comme suit :

Procédure

Étape 1 Activez la journalisation de la mémoire.

memory logging [1024-4194304] [**wrap**] [**size** [1-2147483647]] [**process** *process-name*] [**context** *context-name*]

Exemple :

```
ciscoasa(config)# memory logging 202980
```

Le seul argument requis est le nombre d'entrées dans le tampon de journalisation de la mémoire. L'option **wrap** demande à l'utilitaire de journalisation de la mémoire d'enregistrer le tampon lorsqu'il arrive à saturation. Il ne peut être enregistré qu'une seule fois.

Si le tampon de journalisation de la mémoire arrive à saturation plusieurs fois, il peut être remplacé. Lorsque le tampon arrive à saturation, un déclencheur est envoyé au gestionnaire d'événements pour permettre l'enregistrement des données. L'option **size** surveille une taille particulière. L'option **process** surveille un processus particulier.

Remarque
Le processus CheckHeaps est complètement ignoré en tant que processus, car il utilise l'allocation de mémoire d'une manière non standard.

L'option **context** enregistre la journalisation de la mémoire pour un contexte virtuel donné sous le nom indiqué.

Pour modifier les paramètres de journalisation de la mémoire, vous devez la désactiver, puis la réactiver.

Étape 2 Affichez les résultats de la journalisation de la mémoire.

```
show memory logging [brief | wrap]
show memory logging include [address] [caller] [operator] [size] [process] [time] [context]
```

Exemple :

```
ciscoasa# show memory logging
Number of free                          6
Number of calloc                        0
Number of malloc                        8
```

```
Number of realloc-new                    0
Number of realloc-free                   0
Number of realloc-null                   0
Number of realloc-same                   0
Number of calloc-fail                    0
Number of malloc-fail                    0
Number of realloc-fail                   0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x0000000013193e8
0x0000000000443455 0x0000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
time=[13:26:35.964] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
time=[13:26:38.464] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x0000000013193e8
0x0000000000443455 0x0000000001318f5b

ciscoasa# show memory logging include process operation size
Number of free                           6
Number of calloc                         0
Number of malloc                         8
Number of realloc-new                    0
Number of realloc-free                   0
Number of realloc-null                   0
Number of realloc-same                   0
Number of calloc-fail                    0
Number of malloc-fail                    0
Number of realloc-fail                   0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free]
```

```
size=72 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[CMGR Server Process] oper=[free] size=16 process=[CMGR Server Process]
oper=[free] size=40 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[ci/console] oper=[malloc] size=72 process=[ci/console]
oper=[free] size=72 ciscoasa# show memory logging brief
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

Sans aucun option, **show memory logging** affiche les statistiques, puis les opérations enregistrées. L'option **brief** affiche uniquement les statistiques. L'option **wrap** affiche le tampon lors de l'encapsulation, puis purge les données afin que les données dupliquées n'apparaissent pas ou ne soient pas enregistrées. L'option **include** inclut uniquement les champs spécifiés dans la sortie. Vous pouvez spécifier les champs dans n'importe quel ordre, mais ils s'affichent toujours dans l'ordre suivant :

1. Processus
2. Durée
3. Contexte (sauf en mode unique)
4. Opération (libre/malloc/etc.)
5. Adresse
6. Taille
7. Appelants

Le format de sortie est le suivant :

process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

Jusqu'à quatre adresses d'appelants apparaissent. Les types d'opérations sont répertoriés dans la sortie (nombre de...) illustrée dans l'exemple.

Étape 3 Répondez aux événements d'encapsulation de la mémoire.

event memory-logging-wrap

Exemple :

```
ciscoasa(config)# event manager applet memlog
ciscoasa(config)# event memory-logging-wrap
ciscoasa(config)# action 0 cli command "show memory logging wrap"
ciscoasa(config)# output file append disk0:/memlog.log
```

L'exemple montre un applet qui enregistre toutes les allocations de mémoire. Lorsque l'encapsulation est activée pour la journalisation de la mémoire, le journaliseur de mémoire envoie un événement au gestionnaire d'événements afin de déclencher les applets configurés.

Exemples d'EEG

L'exemple suivant montre un applet de gestionnaire d'événements qui enregistre les renseignements de fuite de bloc toutes les heures et écrit le résultat dans un ensemble rotatif de fichiers journaux, en conservant les journaux d'une journée :

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description "Log block usage"
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command "show blocks old"
```

L'exemple suivant montre un applet de gestionnaire d'événements qui redémarre l'ASA tous les jours à 1 h, en enregistrant la configuration si nécessaire :

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description "Reboot every night"
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "reload save-config noconfirm"
```

L'exemple suivant montre des applets de gestionnaire d'événements qui désactivent l'interface donnée entre minuit et 3 h.

```
ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description "Disable the interface at midnight"
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description "Enable the interface at 3am"
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "no shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"
```

Supervision de l'EEG

Consultez les commandes suivantes pour superviser l'EEG.

- **clear configure event manager**

  Cette commande supprime la configuration en cours d'exécution du gestionnaire d'événements.

- **clear configure event manager applet** *appletname*

  Cette commande supprime l'applet de gestionnaire d'événements nommé de la configuration.

- **show counters protocol eem**

  Cette commande affiche les compteurs du gestionnaire d'événements.

- **show event manager**

  Cette commande affiche des renseignements sur les applets de gestionnaire d'événements configurés, notamment le nombre d'accès et la date de la dernière invocation des applets du gestionnaire d'événements.

- **show memory logging, show memory logging include**

  Ces commandes affichent les statistiques sur les allocations de mémoire et l'utilisation de la mémoire.

- **show running-config event manager**

  Cette commande affiche la configuration en cours d'exécution du gestionnaire d'événements.

Historique de l'EEG

Tableau 59 : Historique de l'EEG

Nom de la caractéristique	Versions de plateforme	Description
Gestionnaire d'événements intégré de Cisco (EEG)	9.2(1)	Le service EEG vous permet de déboguer les problèmes et fournit une journalisation à usage général pour le dépannage. Il y a deux composants : les événements auxquels l'EEG répond ou écoute, et les applets de gestionnaire d'événements qui définissent les actions ainsi que les événements auxquels l'EEG répond. Vous pouvez configurer plusieurs applets de gestionnaire d'événements pour répondre à différents événements et effectuer des actions différentes. Nous avons introduit ou modifié les commandes suivantes : **event manager applet**, **description**, **event syslog id**, **event none**, **event timer** {**watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss*}, **event crashinfo**, **action cli command**, **output** {**none** | **console** | **file** {**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*}}, **show running-config event manager**, **event manager run**, **show event manager**, **show counters protocol eem**, **clear configure event manager**, **debug event manager**, **debug menu eem**.

Nom de la caractéristique	Versions de plateforme	Description
Suivi de mémoire pour l'EEG	9.4(1)	Nous avons ajouté une nouvelle fonctionnalité de débogage pour consigner les allocations de mémoire et l'utilisation de la mémoire, et pour répondre aux événements d'encapsulation de la journalisation de la mémoire. Nous avons introduit ou modifié les commandes suivantes : **memory logging**, **show memory logging**, **show memory logging include**, **event memory-logging-wrap**.



CHAPITRE 46

Tests et dépannage

Ce chapitre décrit comment dépanner l'ASA et tester la connectivité de base.

- Récupérer les mots de passe d'activation et Telnet, à la page 1391
- Afficher les messages de débogage, à la page 1395
- Capture de paquets, à la page 1395
- Afficher le vidage en cas de panne, à la page 1402
- Afficher le vidage de la mémoire, à la page 1402
- Utilisation et rapport d'utilisation du processeur (CPU), à la page 1402
- Tester votre configuration, à la page 1407
- Supervision des connexions, à la page 1420
- Historique des tests et du dépannage , à la page 1420

Récupérer les mots de passe d'activation et Telnet

Si vous oubliez les mots de passe d'activation ou Telnet, vous pouvez les récupérer pour les modèles ASA virtuel et ISA 3000. Vous devez effectuer la tâche à l'aide de l'interface de ligne de commande.

Remarque Pour les autres plateformes, vous ne pouvez pas récupérer les mots de passe perdus. Vous pouvez uniquement restaurer la configuration d'usine par défaut et réinitialiser les mots de passe par défaut. Pour Firepower 4100/9300, consultez le Guide de configuration de FXOS. Pour les autres modèles, consultez le Guide de dépannage de FXOS.

Récupérer les mots de passe sur l'ISA 3000

Pour récupérer les mots de passe des ISA 3000, procédez comme suit :

Procédure

Étape 1 Connectez-vous au port de console de l'ASA.

Étape 2 Mettez l'ASA hors tension, puis rallumez-le.

Étape 3 Après le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à passer en mode ROMMON.

Étape 4 Pour mettre à jour la valeur du registre de configuration, entrez la commande suivante :

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

L'ASA affiche la valeur actuelle du registre de configuration et une liste d'options de configuration. Enregistrez la valeur actuelle du registre de configuration afin de pouvoir la restaurer ultérieurement.

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ...... auto-boot index 1 image in disks
```

Étape 5 Rechargez l'ASA en saisissant la commande suivante :

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

L'ASA charge la configuration par défaut au lieu de la configuration de démarrage.

Étape 6 Accédez au mode d'exécution privilégié en saisissant la commande suivante :

```
ciscoasa# enable
```

Étape 7 Lorsque le mot de passe vous est demandé, appuyez sur **Entrée**.

Le mot de passe est une valeur vide.

Étape 8 Chargez la configuration de démarrage en saisissant la commande suivante :

```
ciscoasa# copy startup-config running-config
```

Étape 9 Accédez au mode de configuration globale en saisissant la commande suivante :

```
ciscoasa# configure terminal
```

Étape 10 Modifiez les mots de passe, au besoin, dans la configuration par défaut en saisissant les commandes suivantes :

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

Étape 11 Chargez la configuration par défaut en saisissant la commande suivante :

```
ciscoasa(config)# no config-register
```

La valeur par défaut du registre de configuration est 0x1. Voir la référence des commandes pour en savoir plus sur le registre de configuration.

Étape 12 Enregistrez les nouveaux mots de passe dans la configuration de démarrage en saisissant la commande suivante :

```
ciscoasa(config)# copy running-config startup-config
```

Récupérer les mots de passe ou les images sur l'ASA virtuel

Pour récupérer les mots de passe ou les images sur l'ASA virtuel, procédez comme suit :

Procédure

Étape 1 Copiez la configuration en cours d'exécution dans un fichier de sauvegarde sur l'ASA virtuel :

copy running-config *nom de fichier*

Exemple :

```
ciscoasa# copy running-config backup.cfg
```

Étape 2 Redémarrez l'ASA virtuel :

reload

Étape 3 Dans le menu GNU GRUB, appuyez sur la flèche vers le bas, choisissez <**filename**> **sans option de chargement de configuration**, puis appuyez sur **Enter** (Entrée). Le nom de fichier est le nom de fichier d'image de démarrage par défaut sur l'ASA virtuel. L'image de démarrage par défaut n'est jamais démarrée automatiquement par la commande **fallback**. Chargez ensuite l'image de démarrage sélectionnée.

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

Exemple :

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

Étape 4 Copiez le fichier de configuration de sauvegarde vers la configuration en cours d'exécution.

copy *nom_de_fichier* **running-config**

Exemple :

```
ciscoasa (config)# copy backup.cfg running-config
```

Étape 5 Réinitialisez le mot de passe.

enable password *password*

Exemple :

```
ciscoasa(config)# enable password cisco123
```

Étape 6 Enregistrez la nouvelle configuration.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Désactiver la récupération du mot de passe pour le matériel ISA 3000

Remarque Vous ne pouvez pas désactiver la récupération du mot de passe sur les modèles ASA virtuel, Secure Firewall.

Pour désactiver la récupération du mot de passe et vous assurer que les utilisateurs non autorisés ne peuvent pas utiliser le mécanisme de récupération du mot de passe pour compromettre l'ASA, procédez comme suit.

Avant de commencer

Sur l'ASA, la commande **no service password-recovery** vous empêche de passer en mode ROMMON avec la configuration intacte. Lorsque vous passez en mode ROMMON, l'ASA vous invite à effacer tous les systèmes de fichiers flash. Vous ne pouvez pas passer en mode ROMMON sans effectuer au préalable cet effacement. Si vous choisissez de ne pas effacer le système de fichiers flash, l'ASA se recharge. Étant donné que la récupération du mot de passe dépend de l'utilisation du mode ROMMON et du maintien de la configuration existante, cet effacement vous empêche de récupérer un mot de passe. Cependant, la désactivation de la récupération du mot de passe empêche les utilisateurs non autorisés d'afficher la configuration ou d'insérer des mots de passe différents. Dans ce cas, pour restaurer le système à un état de fonctionnement, chargez une nouvelle image et un fichier de configuration de sauvegarde, le cas échéant.

La commande **service password-recovery** apparaît dans le fichier de configuration pour information uniquement. Lorsque vous saisissez la commande à l'invite de l'interface de ligne de commande, le paramètre est enregistré dans la NVRAM. La seule façon de modifier le paramètre est d'entrer la commande à l'invite de l'interface de ligne de commande. Le chargement d'une nouvelle configuration avec une version différente de la commande ne modifie pas le paramètre. Si vous désactivez la récupération du mot de passe lorsque l'ASA est configuré pour ignorer la configuration de démarrage au démarrage (en préparation de la récupération du mot de passe), l'ASA modifie le paramètre pour charger la configuration de démarrage comme d'habitude. Si vous utilisez le basculement et que l'unité de secours est configurée pour ignorer la configuration de démarrage, la même modification est apportée au registre de configuration lorsque la commande **no service password- recovery** est dupliquée sur l'unité de secours.

Procédure

Désactivez la récupération du mot de passe.

no service password-recovery

Exemple :

```
ciscoasa (config)# no service password-recovery
```

Afficher les messages de débogage

Comme les résultats du débogage obéissent à un niveau de priorité élevé dans le processus du CPU, ils sont susceptibles de rendre le système inutilisable. Par conséquent, les commandes **debug** doivent uniquement être utilisées pour résoudre des problèmes spécifiques ou au cours de sessions de dépannage effectuées avec le personnel d'assistance technique de Cisco. De plus, il est préférable d'utiliser les commandes **debug** en dehors des périodes d'affluence de trafic et lorsque peu d'utilisateurs sont connectés au réseau. En effectuant le débogage pendant ces périodes, il y moins de chance que des frais généraux d'administration accrus associés à l'exécution de la commande **debug** aient des répercussions sur l'utilisation du système. Pour activer les messages de débogage, consultez les commandes **debug** dans la référence de commande.

Capture de paquets

La capture de paquets peut être utile lors du dépannage de problèmes de connectivité ou de la surveillance d'activités suspectes. Nous vous conseillons de communiquer avec le TAC de Cisco si vous souhaitez utiliser le service de capture de paquets.

Lignes directrices pour la capture des paquets

Mode contextuel

- Vous pouvez configurer les captures sur la liaison de commande de grappe dans un contexte; seul le paquet associé au contexte envoyé dans la liaison de commande de grappe est capturé.
- Vous ne pouvez configurer qu'une seule capture pour un VLAN partagé; si vous configurez une capture dans plusieurs contextes sur le VLAN partagé, seule la dernière capture configurée est utilisée.
- Si vous supprimez la dernière capture configurée (active), aucune capture ne devient active, même si vous avez déjà configuré une capture dans un autre contexte; vous devez supprimer la capture et l'ajouter à nouveau pour la rendre active.
- Tout le trafic qui entre dans l'interface à laquelle la capture est connectée est capturé, y compris le trafic vers d'autres contextes sur le VLAN partagé. Par conséquent, si vous activez une capture dans le contexte A pour un VLAN qui est également utilisé par le contexte B, le trafic entrant du contexte A et du contexte B est capturé.

- Pour le trafic de sortie, seul le trafic du contexte avec la capture active est capturé. La seule exception est lorsque vous n'activez pas l'inspection ICMP (par conséquent, le trafic ICMP n'a pas de session dans le chemin accéléré). Dans ce cas, le trafic ICMP d'entrée et de sortie pour tous les contextes sur le VLAN partagé est capturé.

Directives supplémentaires

- Si l'ASA reçoit des paquets avec un en-tête TCP mal formaté et les abandonne du fait de la raison d'abandon ASP *invalid-tcp-hdr-length*, la sortie de la commande **show capture** sur l'interface où ces paquets sont reçus n'affiche pas ces paquets.
- Vous pouvez uniquement capturer le trafic IP; vous ne pouvez pas capturer des paquets non IP tels que les ARP.
- Pour les paquets marqués SGT en ligne, les paquets capturés contiennent un en-tête CMD supplémentaire que votre visualiseur PCAP pourrait ne pas comprendre.
- Les captures de paquets comprennent les paquets que le système modifie ou injecte dans la connexion en raison de l'inspection, de la normalisation de la NAT, du TCP ou d'autres fonctionnalités qui ajustent le contenu d'un paquet.
- La trace de la durée de vie d'un paquet virtuel injecté dans un chemin de données ne reflète pas exactement la façon dont le chemin de données gère les paquets physiques. Cette différence dépend de la version du logiciel, de la configuration et du type de paquets virtuels injectés. Voici les paramètres de configuration qui pourraient entraîner cette disparité :
  - Il existe au moins 2 instructions NAT pour le même hôte.
  - Les flux avant et arrière d'une connexion ont des protocoles différents. Par exemple, le flux avant est UDP ou TCP, le flux arrière est ICMP.
  - L'inspection d'erreurs ICMP est activée.

Capturer les paquets

Pour capturer des paquets, procédez comme suit.

Procédure

Étape 1 Activez les fonctionnalités de capture de paquets pour l'analyse de paquets et l'isolement des défaillances de réseau :

capture *capture_name* [**type** {**asp-drop** [**all** | *drop-code*] | **tls-proxy** | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] {**interface** {*interface_name* | **asa_dataplane** | **asa_mgmt_plane** | **cplane**} } [**buffer** *buf_size*] [**ethernet-type** *type*] [**reeinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**file-size**] [**headers-only**] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

Exemple :

```
ciscoasa# capture captest interface inside
```

Vous devez configurer une interface pour capturer tous les paquets. Utilisez le même *capture_name* sur plusieurs instructions **capture** pour capturer plusieurs types de trafic.

Le mot clé **type asp-drop** capture les paquets abandonnés par le chemin de sécurité accélérée. Dans une grappe, les paquets de données abandonnés d'une unité à une autre sont également capturés. En mode de contexte multiple, lorsque cette option est activée dans l'espace d'exécution du système, tous les paquets de données abandonnés sont capturés; lorsque cette option est émise dans un contexte, seuls les paquets de données abandonnés qui proviennent d'interfaces appartenant à ce contexte sont capturés.

Les mots clés **type raw-data** capturent les paquets entrants et sortants. Il s'agit du paramètre par défaut.

La paire mot clé-argument **inline-tag** *tag* spécifie une balise pour une valeur SGT particulière ou la laisse non spécifiée pour capturer un paquet étiqueté avec n'importe quelle valeur SGT.

Le mot clé **buffer** définit la taille de la mémoire tampon utilisée pour stocker le paquet. Lorsque la mémoire tampon d'octets est pleine, la capture de paquets s'arrête. Lorsqu'elle est utilisée dans une grappe, il s'agit de la taille par unité, et non de la somme de toutes les unités. Le mot clé **circular-buffer** remplace la mémoire tampon, en commençant par le début, lorsqu'elle est pleine.

Le mot clé **ethernet-type** définit un type Ethernet à capturer. Les types Ethernet pris en charge comprennent 8021Q, ARP, IP, IP6, LACP, PPPOED, PPPOES, RARP et VLAN. Une exception se produit avec le type 802.1Q ou VLAN. La balise 802.1Q est automatiquement ignorée et le type Ethernet interne est utilisé pour la mise en correspondance. L'IP est le type Ethernet par défaut.

Le mot clé **interface** définit le nom de l'interface sur laquelle utiliser la capture de paquets.

Pour capturer des paquets dans le plan de données, utilisez le mot clé **asa_dataplane**.

Pour configurer la taille du fichier de capture, utilisez le mot clé **file-size**. La taille du fichier peut être comprise entre 32 et 10 000 Mo.

Si vous souhaitez capturer uniquement les en-têtes de paquet L2, L3 et L4 sans données, utilisez la commande **headers-only** .

Le mot clé **match** capture la correspondance du protocole, des adresses IP source et de destination et des ports facultatifs. Vous pouvez utiliser ce mot clé jusqu'à trois fois dans une même commande. Le mot clé **any** capture uniquement le trafic IPv4. Vous pouvez utiliser les mots clés **any4** et **any6** pour capturer le trafic réseau IPv4 et IPv6 correspondant, respectivement. L'opérateur peut être l'une des options suivantes :

- lt : inférieur à
- gt : supérieur à
- eq : égal à

Le mot clé **real-time** affiche les paquets capturés en permanence en temps réel.

Le mot clé **reinject-hide** spécifie qu'aucun paquet réinjecté ne sera capturé et s'applique uniquement dans un environnement de mise en grappe.

Remarque
Si l'optimisation ACL est configurée, vous ne pouvez pas utiliser la commande **access-list** dans la capture. Vous ne pouvez utiliser que la commande **access-group**. Une erreur s'affiche si vous essayez d'utiliser la commande **access-list** dans ce cas.

Étape 2 Capturez le trafic de liaison de commande de la grappe :

capture *capture_name* {**type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]]

capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**cp-cluster**] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

Exemple :

```
ciscoasa# capture ccl type lacp interface GigabitEthernet0/0
ciscoasa# capture ccl interface cluster match udp any eq 49495 any
ciscoasa# capture ccl interface cluster match udp any any eq 49495
```

Vous pouvez capturer le trafic de liaison de commande de grappe de deux manières : pour capturer tout le trafic sur la liaison de commande de grappe, utilisez le mot clé **cluster** pour le nom de l'interface. Pour capturer uniquement les paquets cLACP, spécifiez **type lacp**, puis indiquez l'ID de l'interface physique au lieu du nom de l'interface. Il existe deux types de paquets sur la liaison de commande de grappe : les paquets de plan de commande et les paquets de plan de données, qui comprennent tous deux le trafic de données transféré et les messages LU de la grappe. Le champ TTL de l'en-tête d'adresse IP est codé pour différencier ces deux types de paquets. Lorsque des paquets de données transférés sont capturés, leurs terminaisons de mise en grappe sont incluses dans le fichier de capture à des fins de débogage.

Le mot clé **cp-cluster** ne capture que les paquets du plan de commande sur la liaison de commande de grappe (et aucun paquet de plan de données). Cette option est utile dans le système en mode de contexte multiple où vous ne pouvez pas faire correspondre le trafic à l'aide d'une liste de contrôle d'accès.

Étape 3 Capturez les paquets à l'échelle de la grappe :

cluster exec capture *capture_name arguments*

Étape 4 Arrêtez la capture de paquets :

no capture *capture_name*

Pour terminer une capture de paquets en temps réel, utilisez les touches **Ctrl + c.** Pour supprimer définitivement la capture, utilisez la forme **no** (non) de cette commande. L'option en temps réel s'applique uniquement aux captures **raw-data** et **asp-drop**.

Étape 5 Pour arrêter manuellement la capture de paquets sans supprimer les paquets de la mémoire tampon :

capture *nom* **stop**

Étape 6 Pour redémarrer la capture :

no capture *nom***stop**

Étape 7 Capturez les traces de paquet persistantes sur les unités de grappe :

cluster exec *capture_test* **persist**

Étape 8 Effacez les traces de paquet persistantes :

cluster exec *clear* **packet-trace**

Étape 9 Capturez les paquets IPsec déchiffrés :

cluster exec *capture_test* **include-decrypted**

Étape 10 Effacez la capture :

clear capture *capture_name*

Exemples

Paquets du plan de commande

Tous les paquets vers et depuis le plan de commande ont une TTL de 255, et le numéro de port 49495 est utilisé pour le port d'écoute du plan de commande de la mise en grappe. L'exemple suivant montre comment créer une capture LACP pour l'environnement de mise en grappe :

```
ciscoasa# capture lacp type lacp interface GigabitEthernet0/0
```

L'exemple suivant montre comment créer une capture pour les paquets du chemin de commande dans la liaison de mise en grappe :

```
ciscoasa# capture cp interface cluster match udp any eq 49495 any
ciscoasa# capture cp interface cluster match udp any any eq 49495
```

Paquets du plan de données

Les paquets de données comprennent ceux transférés d'une unité à l'autre (son propriétaire de connexion) et les messages LU de la grappe. Les messages de mises à jour LU régulières de la grappe ont une TTL de 254, et il existe un paquet LU spécial qui a une TTL de 253. Ce paquet LU spécial est uniquement pour TCP et il ne se produit que lorsque le directeur choisit un nouveau propriétaire de flux; le directeur renvoie le paquet demandé avec le paquet de mise à jour CLU_FULL. Le paquet LU est rempli avec l'en-tête L3/L4 du paquet d'origine pour éviter une situation de concurrence potentielle du côté du récepteur. Les paquets de données transférés ont une TTL inférieure à 4. L'exemple suivant montre comment créer une capture pour les paquets du chemin de données dans la liaison de commande de grappe : Pour capturer tous les messages de « flow logical update » (mise à jour logique du flux) du plan de données inter-grappes, utilisez le port 4193.

```
ciscoasa# access-list cc1 extended permit udp any any eq 4193
ciscoasa# access-list cc1 extended permit udp any eq 4193 any
ciscoasa# capture dp interface cluster access-list ccl
```

Afficher une capture de paquets

Vous pouvez afficher une capture de paquet au niveau de l'interface de ligne de commande, dans un navigateur, ou télécharger une capture sur un serveur de votre choix.

Procédure

Étape 1 Affichez la capture sur l'interface de ligne de commande :

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

Exemple :

```
ciscoasa# show capture capin

 8 packets captured

 1: 03:24:35.526812       192.168.10.10 > 203.0.113.3: icmp: echo request
 2: 03:24:35.527224       203.0.113.3 > 192.168.10.10: icmp: echo reply
 3: 03:24:35.528247       192.168.10.10 > 203.0.113.3: icmp: echo request
 4: 03:24:35.528582       203.0.113.3 > 192.168.10.10: icmp: echo reply
 5: 03:24:35.529345       192.168.10.10 > 203.0.113.3: icmp: echo request
 6: 03:24:35.529681       203.0.113.3 > 192.168.10.10: icmp: echo reply
 7: 03:24:57.440162       192.168.10.10 > 203.0.113.3: icmp: echo request
 8: 03:24:57.440757       203.0.113.3 > 192.168.10.10: icmp: echo reply
```

Le mot clé **access-list** affiche des renseignements sur les paquets basés sur l'adresse IP ou les champs supérieurs pour l'identification de la liste d'accès spécifique.

Le mot clé **cluster exec** vous permet d'émettre la commande **show capture** sur une unité et d'exécuter la commande sur toutes les autres unités en même temps.

Le mot clé **count** affiche le nombre de paquets de données spécifiés.

Le mot clé **decode** est utile lorsqu'une capture de type **isakmp** est appliquée à une interface. Toutes les données ISAKMP passant par cette interface seront capturées après le déchiffrement et affichées avec plus de renseignements après le décodage des champs. La sortie décodée des paquets dépend du protocole du paquet. Généralement, cette commande prend en charge le décodage IP pour les protocoles ICMP, UDP et TCP. À partir de la version 9.10(1), cette commande prend également en charge le décodage IP pour GRE et IPinIP.

Le mot clé **detail** affiche des renseignements supplémentaires sur le protocole pour chaque paquet.

Le mot clé **dump** affiche un vidage hexadécimal des paquets transportés sur la liaison de données.

Le mot clé **packet-number** commence l'affichage au numéro de paquet spécifié.

Étape 2 Affichez la capture de paquets dans votre navigateur :

https://*ip_of_asa***/admin/capture/***capture_name***/pcap**

Si vous omettez le mot clé **pcap**, seul l'équivalent de la sortie de la commande **show capture** *capture_name* est fourni.

En mode de contexte multiple, la commande **copy capture** est disponible seulement dans l'espace d'exécution du système.

Étape 3 Copiez la capture de paquets sur un serveur. Cet exemple montre le serveur FTP.

[**cluster exec**] **copy /pcap capture:**[*context-name/*]*capture_name* **ftp://***username***:***password***@***server_ip***/***path*

Si vous omettez le mot clé **pcap**, seul l'équivalent de la sortie de la commande **show capture** *capture_name* est fourni.

Remarque

Lorsque vous copiez une capture de paquets sur un disque, assurez-vous que le nom de fichier de la capture est inférieur ou égal à 63 caractères. Lorsque le nom de fichier comporte plus de 63 caractères, bien que la capture de paquets soit réussie, la copie de la capture sur un disque échoue.

Exemples

L'exemple suivant montre une capture de type asp-drop :

```
ciscoasa# capture asp-drop type asp-drop acl-drop
ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown

ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown
```

L'exemple suivant montre une capture de type Ethernet :

```
ciscoasa# capture arp ethernet-type arp interface inside
ciscoasa# show cap arp

22 packets captured

   1: 05:32:52.119485       arp who-has 10.10.3.13 tell 10.10.3.12
   2: 05:32:52.481862       arp who-has 192.168.10.123 tell 192.168.100.100
   3: 05:32:52.481878       arp who-has 192.168.10.50 tell 192.168.100.10
   4: 05:32:53.409723       arp who-has 10.106.44.135 tell 10.106.44.244
   5: 05:32:53.772085       arp who-has 10.106.44.108 tell 10.106.44.248
   6: 05:32:54.782429       arp who-has 10.106.44.135 tell 10.106.44.244
   7: 05:32:54.784695       arp who-has 10.106.44.1 tell 11.11.11.112:
```

Afficher le vidage en cas de panne

Si l'ASA ou l'ASA virtuel tombe en panne, vous pouvez afficher les renseignements de vidage en cas de panne. Nous vous conseillons de communiquer avec le TAC de Cisco si vous souhaitez interpréter le vidage en cas de panne. Consultez la commande **show crashdump** dans la référence de commande.

Afficher le vidage de la mémoire

Un vidage de la mémoire est un instantané du programme en cours d'exécution lorsque celui-ci s'est terminé de façon anormale ou a planté. Les vidages de la mémoire sont utilisés pour diagnostiquer ou déboguer les erreurs et enregistrer un plantage en vue d'une analyse hors site ultérieure. Le TAC de Cisco peut vous demander d'activer la fonction de vidage de la mémoire pour résoudre les pannes d'application ou de système sur l'ASA ou ASA virtuel. Consultez la commande **coredump** dans la référence de commande.

Utilisation et rapport d'utilisation du processeur (CPU)

Le rapport d'utilisation du processeur résume le pourcentage du processeur utilisé pendant la période précisée. En règle générale, le cœur fonctionne à environ 30 à 40 % de la capacité totale du processeur en dehors des heures de pointe et à environ 60 à 70 % de capacité pendant les heures de pointe.

Utilisation de vCPU dans l'ASA virtuel

Utilisez la commande **show cpu usage** sur l'ASA virtuel pour afficher les statistiques d'utilisation du processeur. L'utilisation de vCPU dans ASA virtuel affiche la quantité de vCPU utilisée pour le chemin de données, le point de contrôle et les processus externes.

L'utilisation de vCPU signalée par le fournisseur de services en nuage (comme VMware, Azure, OCI, etc.) comprend l'utilisation de l'ASA virtuel comme décrit plus :

- Temps d'inactivité d'ASA virtuel
- %SYS surdébit utilisé pour la VM ASA virtuel
- Surdébit du déplacement des paquets entre les vSwitches, les vNIC et les pNIC. Ce surdébit peut être assez important.

Exemple d'utilisation du processeur

Voici un exemple dans lequel l'utilisation de vCPU signalée est sensiblement différente :

- Rapports ASA virtuel : 40 %
- DP : 35 %
- Processus externes : 5 %
- Rapports vSphere : 95 %
- ASA (comme les rapports ASA virtuel) : 40 %

- Interrogation ASA inactive : 10 %
- Frais généraux : 45 %

Le surdébit est utilisé pour effectuer des fonctions d'hyperviseur et pour déplacer des paquets entre les NIC et les vNIC à l'aide du vSwitch.

L'utilisation peut dépasser 100 %, car le serveur ESXi peut utiliser des ressources de traitement supplémentaires pour le surdébit au nom de l'ASA virtuel.

Rapport d'utilisation du CPU VMware

Dans vSphere, cliquez sur l'onglet **VM Performance** (Performances de la VM), puis sur **Advanced** (Avancé) pour afficher la liste déroulante **Chart Options** (Options du graphique), qui indique l'utilisation de vCPU pour chaque état (%Utilisateur, %Inactif, %Sys, etc.) de la VM. Ces renseignements sont utiles pour comprendre le point de vue de VMware sur l'utilisation des ressources de CPU.

Sur l'interface shell du serveur ESXi (vous accédez à l'interface shell en utilisant SSH pour vous connecter à l'hôte), esxtop est disponible. Esxtop a une apparence similaire à la commande **top** de Linux et fournit des renseignements sur l'état de la VM pour les performances de vSphere, notamment les suivantes :

- Détails sur l'utilisation du vCPU, de la mémoire et du réseau
- Utilisation du vCPU pour chaque état de chaque VM.
- Mémoire (type M pendant l'exécution) et réseau (type N pendant l'exécution), ainsi que les statistiques et le nombre d'abandons RX

ASA virtuel et graphiques vCenter

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et vCenter :

- Les numéros de graphique vCenter sont toujours supérieurs aux numéros d'ASA virtuel.
- vCenter l'appelle « %CPU usage » (% d'usage du CPU); l'ASA virtuel l'appelle « %CPU utilization » (% d'utilisation du CPU).

Les termes « %CPU utilization » et « %CPU usage » ont des significations différentes :

- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

vCenter calcule le pourcentage d'usage du CPU comme suit :

Nombre de processeur (CPU) virtuels utilisés activement, spécifié en pourcentage du nombre total de CPU disponibles

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'usage du CPU virtuel est l'usage en MHz/nombre de CPU virtuels x fréquence du cœur

Lorsque vous comparez l'utilisation en MHz, les chiffres de vCenter et d'ASA virtuel correspondent. Selon le graphique vCenter, l'utilisation du CPU en % MHz est calculée comme suit : 60/(2499 x 1 vCPU) = 2,4

Rapports d'utilisation du CPU Amazon CloudWatch

Vous pouvez afficher l'explorateur de mesures pour surveiller les ressources en fonction de leurs balises et de leurs propriétés. Procédez comme suit pour afficher les statistiques d'utilisation du processeur pour une instance en particulier :

Procédure

Étape 1 Ouvrez la console **CloudWatch** et choisissez **Metrics** (Mesures) dans le volet de navigation.

Étape 2 Sélectionnez l'espace de noms de la mesure **EC2** et sélectionnez la dimension **Per-instance Metrics** (Mesures par instance).

Étape 3 Saisissez **CPU Utilization** (Utilisation du CPU) dans le champ de recherche et appuyez sur Entrée. Sélectionnez la ligne de l'instance requise pour afficher un graphique de la mesure **CPU Utilization** (Utilisation du CPU) pour cette instance.

Pour en savoir plus, consultez la documentation relative à Amazon CloudWatch.

ASA virtuel et graphiques Amazon CloudWatch

Les chiffres du graphique Amazon CloudWatch sont supérieurs aux chiffres réels en raison des différentes façons de calculer l'utilisation du CPU sur l'ASA virtuel et le CloudWatch.

Lorsque l'ASA virtuel fonctionne en mode d'interrogation, chaque CPU exécute une boucle de commandes allégées au lieu d'entrer en mode d'économie d'alimentation ou dans tout autre état inactif. Cela améliore les performances en maintenant chaque cœur actif en tout temps au lieu de devoir l'activer/le désactiver ou que leurs horloges soient ajustées en fonction des états d'alimentation Intel.

À l'intérieur de l'ASA virtuel, cette activité est comprise comme un comportement inactif et l'utilisation du CPU est correctement calculée. Cependant, sur Amazon CloudWatch, le comportement inactif ressemble à une activité normale du CPU, car tous les cycles du CPU ont des instructions à exécuter, ce qui conduit le CloudWatch à afficher un pourcentage d'utilisation du CPU élevé (85 à 90 %).

Rapport d'utilisation du CPU Azure

Effectuez les étapes suivantes pour afficher le % d'utilisation du CPU sur toutes les VM surveillées à l'aide des observations VM du moniteur Azure :

Procédure

Étape 1 Accédez au portail Azure, sélectionnez **Monitor** (Superviser) et choisissez **Virtual Machines** (Machines virtuelles) dans la section **Solutions**.

Étape 2 Sélectionnez l'onglet **Performance** pour afficher le tableau **CPU Utilization %** (% d'utilisation du CPU). Ce tableau affiche les cinq machines ayant la plus forte utilisation moyenne du processeur.

Effectuez les étapes suivantes pour afficher le tableau du % d'utilisation du CPU directement à partir d'une machine virtuelle Azure spécifique :

Procédure

Étape 1 Accédez au portail Azure et sélectionnez **Virtual Machines** (Machines virtuelles).

Étape 2 Dans la liste des VM, choisissez une VM.

Étape 3 Dans la section **Monitoring** (Supervision), sélectionnez **Insights** (Observations).

Étape 4 Sélectionnez l'onglet **Performance**.

Consultez la section Comment représenter graphiquement les performances avec les observations VM pour en savoir plus.

Graphiques ASA virtuel et Azure

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et Azure. Les numéros du graphique Azure sont toujours supérieurs aux numéros de l'ASA virtuel, car Azure calcule l'utilisation en % du CPU comme la quantité de CPU virtuels utilisés activement, spécifié en pourcentage du total des CPU disponibles.

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'utilisation du CPU virtuel est l'utilisation en MHz/nombre de CPU virtuels x fréquence du cœur.

Azure limite également la quantité de CPU demandée par le système d'exploitation invité. Imaginez un scénario dans lequel l'ASA virtuel signale une utilisation du CPU à 40 % et l'hyperviseur signale une utilisation du CPU à 90 %. Maintenant, si l'ASA virtuel a besoin de plus de puissance de traitement, l'utilisation du CPU peut dépasser 80 % et l'hyperviseur peut alors signaler l'utilisation du CPU à plus de 95 %. Cela conduit l'hyperviseur à limiter le CPU de l'ASA virtuel même si l'ASA virtuel n'exécute qu'une boucle de commandes légères en mode d'interrogation et présente un comportement inactif.

Rapport d'utilisation du CPU Hyper-V

En plus d'afficher les renseignements de configuration du CPU, de la RAM et de l'espace disque pour les serveurs en nuage disponibles, vous pouvez également afficher les renseignements sur le disque, les E/S et le réseau. Utilisez ces renseignements pour vous aider à décider quel serveur en nuage correspond à vos besoins. Vous pouvez afficher les serveurs disponibles par le biais du client nova de ligne de commande ou de l'interface du **panneau de commande en nuage**.

Dans la ligne de commande, exécutez la commande suivante :

```
nova flavor-list
```

Toutes les configurations de serveur disponibles sont affichées. La liste contient les renseignements suivants :

- ID – ID de configuration du serveur
- Name – nom de la configuration, étiqueté par taille de RAM et type de performance
- Mémoire_Mo – la quantité de RAM pour la configuration
- Disque – la taille du disque en Go (pour les serveurs en nuage à usage général, la taille du disque système)
- Éphémère – la taille du disque de données
- Permutation – la taille de l'espace de permutation
- VCPU – le nombre de CPU virtuels associés à la configuration
- Facteur_RXTX – la quantité de bande passante, en Mbit/s, allouée aux ports PublicNet, aux ports ServiceNet et aux réseaux isolés (réseaux en nuage) reliés à un serveur.
- Est_Public – non utilisé

Graphiques ASA virtuel et Hyper-V

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et Hyper-V :

- Les numéros de graphique Hyper-V sont toujours supérieurs aux numéros d'ASA virtuel.
- Hyper-V l'appelle « %CPU usage » (% d'usage du CPU); l'ASA virtuel l'appelle « %CPU utilization » (% d'utilisation du CPU).

Les termes « %CPU utilization » et « %CPU usage » ont des significations différentes :

- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

Hyper-V calcule le pourcentage d'usage du CPU comme suit :

Nombre de processeur (CPU) virtuels utilisés activement, spécifié en pourcentage du nombre total de CPU disponibles

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'usage du CPU virtuel est l'usage en MHz/nombre de CPU virtuels x fréquence du cœur



Remarque Il est conseillé de consulter les rapports d'ASA virtuel pour obtenir un pourcentage d'usage précis du processeur.

Rapport d'utilisation du CPU OCI

Vous pouvez afficher le % d'utilisation du processeur dans le protocole OCI à l'aide de la mesure d'instance de calcul : **oci_computeagent**. La mesure d'utilisation du CPU affiche le niveau d'activité du CPU et est exprimée en pourcentage de temps total. Effectuez les étapes suivantes pour afficher les tableaux de mesures pour une seule instance de calcul :

Procédure

Étape 1 Ouvrez le menu de navigation et cliquez sur **Instances** sous **Compute** (Calcul).

Étape 2 Cliquez sur une instance, puis sur **Metrics** (Mesures) sous **Resources** (Ressources).

Étape 3 Sélectionnez **oci_computeagent** dans la liste Metric namespace (Espace de noms de mesures).

Consultez la section Mesures des instances de calcul pour en savoir plus.

ASA virtuel et graphiques OCI

Les numéros du graphique OCI sont toujours supérieurs aux numéros de l'ASA virtuel, car l'OCI calcule l'utilisation en % du CPU comme la quantité de CPU virtuels utilisés activement, spécifié en pourcentage du total des CPU disponibles.

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'utilisation du CPU virtuel est l'utilisation en MHz/nombre de CPU virtuels x fréquence du cœur.

Tester votre configuration

Cette section décrit comment tester la connectivité pour l'ASA en mode unique ou pour chaque contexte de sécurité, comment envoyer un message Ping aux interfaces ASA et comment autoriser les hôtes d'une interface à envoyer un message Ping aux hôtes sur une autre interface.

Tester la connectivité de base : envoi d'un ping à des adresses

Ping est une commande simple qui vous permet de déterminer si une adresse particulière est active et réactive. Les rubriques suivantes fournissent des renseignements supplémentaires sur la commande et les types de tests que vous pouvez effectuer avec celle-ci.

Ce que vous pouvez tester en utilisant le ping

Lorsque vous envoyez un message Ping à un périphérique, un paquet est envoyé à ce dernier, qui renvoie une réponse. Ce processus permet aux périphériques réseau de se détecter, de s'identifier et de se tester mutuellement.

Vous pouvez utiliser les messages Ping pour effectuer les tests suivants :

- Test de boucle avec retour de deux interfaces : vous pouvez initier l'envoi d'un message Ping d'une interface à une autre sur le même ASA, en tant que test de boucle avec retour externe pour vérifier l'état « opérationnel » de base et le fonctionnement de chaque interface.
- Envoyer un message Ping à un ASA : vous pouvez envoyer un message Ping à une interface sur un autre ASA pour vérifier qu'il est opérationnel et qu'il répond.
- Envoyer un message Ping via un ASA : vous pouvez envoyer un message Ping via un ASA intermédiaire en effectuant un Ping vers un périphérique situé de l'autre côté de l'ASA. Les paquets traverseront deux interfaces ASA intermédiaires dans chaque direction. Cette action effectue un test de base des interfaces, du fonctionnement et du temps de réponse de l'unité intermédiaire.
- Envoyer un message Ping pour tester le fonctionnement suspect d'un appareil réseau : vous pouvez envoyer un message Ping d'une interface ASA vers un appareil réseau que vous soupçonnez de fonctionner de manière incorrecte. Si l'interface est configurée correctement et qu'aucun écho n'est reçu, il pourrait y avoir des problèmes avec l'appareil.
- Envoyer un message Ping pour tester les communications intermédiaires : vous pouvez envoyer un message Ping à partir d'une interface ASA vers un appareil réseau connu pour fonctionner correctement. Si l'écho est reçu, le bon fonctionnement de tous les appareils intermédiaires et la connectivité physique sont confirmés.

Choisir entre le ping ICMP et TCP

L'ASA comprend le Ping traditionnel, qui envoie des paquets de requête d'écho ICMP et reçoit les paquets de réponse d'écho en retour. Il s'agit d'un outil standard qui fonctionne bien si tous les périphériques du réseau autorisent le trafic ICMP. Avec le Ping ICMP, vous pouvez envoyer un message Ping aux adresses IPv4 ou IPv6, ou aux noms d'hôte.

Cependant, certains réseaux interdisent le protocole ICMP. Si cela est le cas pour votre réseau, vous pouvez plutôt utiliser le Ping TCP pour tester la connectivité du réseau. Avec le Ping TCP, le Ping envoie des paquets TCP SYN et considère le Ping comme réussi s'il reçoit un SYN-ACK en réponse. Avec le Ping TCP, vous pouvez envoyer un message Ping à des adresses IPv4 ou à des noms d'hôte, mais vous ne pouvez pas envoyer un message Ping à des adresses IPv6.

Gardez à l'esprit qu'un message Ping ICMP ou TCP réussi signifie simplement que l'adresse que vous utilisez est active et répond à ce type de trafic. Cela signifie que la connectivité de base fonctionne. D'autres politiques exécutées sur un périphérique peuvent empêcher des types de trafic de passer avec succès par un périphérique.

Activer le protocole ICMP

Par défaut, vous pouvez envoyer un message Ping d'une interface à haute sécurité vers une interface à faible sécurité. Il vous suffit d'activer l'inspection ICMP pour permettre le trafic de retour. Si vous souhaitez effectuer un message Ping depuis une interface moins sécurisée vers une interface hautement sécurisée, vous devez appliquer une ACL pour autoriser le trafic.

Lors de l'envoi d'un message Ping à une interface ASA, toutes les règles ICMP appliquées à l'interface doivent autoriser les paquets de requête d'écho et de réponse d'écho. Les règles ICMP sont facultatives : si vous ne les configurez pas, tout le trafic ICMP vers une interface est autorisé.

Cette procédure explique toute la configuration ICMP que vous pourriez devoir effectuer pour activer l'envoi d'un message Ping ICMP des interfaces ASA ou pour l'envoi d'un message Ping par l'intermédiaire d'un ASA.

Procédure

Étape 1 Assurez-vous que les règles ICMP autorisent la requête d'écho/la réponse d'écho.

Les règles ICMP sont facultatives et s'appliquent aux paquets ICMP envoyés directement à une interface. Si vous n'appliquez pas de règles ICMP, tous les accès ICMP sont autorisés. Dans ce cas, aucune action n'est requise.

Cependant, si vous mettez en œuvre des règles ICMP, assurez-vous d'inclure au moins les éléments suivants sur chaque interface, en remplaçant « inside » par le nom d'une interface sur votre périphérique.

```
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo inside
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo-reply inside
```

Étape 2 Assurez-vous que les critères d'accès autorisent le protocole ICMP.

Lors de l'envoi d'un message Ping à un hôte via un ASA, les critères d'accès doivent autoriser le trafic ICMP à sortir et à revenir. Le critère d'accès doit autoriser au moins les paquets ICMP de requête d'écho/réponse d'écho. Vous pouvez ajouter ces règles en tant que règles globales.

En supposant que vous avez déjà des critères d'accès appliqués aux interfaces ou appliqués globalement, ajoutez simplement ces règles à l'ACL appropriée, par exemple :

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any anyecho

ciscoasa(config)# access-list outside_access_in extendedpermit icmp any
anyecho-reply
```

Sinon, autorisez tous les ICMP :

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any any
```

Si vous n'avez pas de critères d'accès, vous devrez également autoriser l'autre type de trafic souhaité, car l'application de critères d'accès à une interface ajoute un refus implicite, de sorte que tout autre trafic sera abandonné. Utilisez la commande **access-group** pour appliquer l'ACL à une interface ou globalement.

Si vous ajoutez simplement la règle à des fins de test, vous pouvez utiliser la forme **no** (non) de la commande **access-list** pour supprimer la règle de l'ACL. Si l'ACL complète sert simplement à des fins de test, utilisez la commande **no access-group** pour supprimer l'ACL de l'interface.

Étape 3 Activez l'inspection ICMP.

L'inspection ICMP est nécessaire lors de l'envoi d'un message Ping à l'ASA, par opposition à l'envoi d'un message Ping à une interface. L'inspection permet de renvoyer le trafic (c'est-à-dire le paquet de réponse d'écho) à l'hôte qui a initié le message Ping et garantit également qu'il y a une réponse par paquet, ce qui empêche certains types d'attaques.

Vous pouvez simplement activer l'inspection ICMP dans la politique d'inspection globale par défaut.

```
ciscoasa(config)# policy-map  global_policy
```

```
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
```

Envoyer un message ping à des hôtes

Pour envoyer un message Ping à n'importe quel appareil, vous devez simplement saisir **ping** avec l'adresse IP ou le nom d'hôte, par exemple **ping 10.1.1.1** ou **ping www.exemple.com**. Pour le ping TCP, vous devez inclure le mot clé **tcp** et le port de destination, par exemple **ping tcp www.exemple.com 80**. C'est généralement tout ce que vous avez à faire pour effectuer un test.

Exemple de sortie pour un envoyer un message Ping réussi :

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Si l'envoi d'un message Ping échoue, la sortie indique ? pour chaque tentative en échec, et le taux de réussite est inférieur à 100 % (un échec complet correspond à 0 %) :

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Cependant, vous pouvez également ajouter des paramètres pour contrôler certains aspects du message Ping. Voici vos options de base :

- Ping ICMP.

  ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

  Lieu :

  - *if_name* spécifie l'adresse IP source pour l'envoi d'un message Ping; cependant, l'interface de sortie est déterminée par une recherche de routage à l'aide de la table de routage des données.
  - *host* est le nom IPv4, IPv6 ou le nom d'hôte de l'hôte à qui vous envoyez un message Ping.
  - **repeat** *count* est le nombre de paquets à envoyer. La valeur par défaut est égale à 5.
  - **timeout** *seconds* est le nombre de secondes d'expiration de chaque paquet si aucune réponse n'est reçue. La valeur par défaut est 2.
  - **data** *pattern* est le modèle hexadécimal à utiliser dans les paquets envoyés. La valeur par défaut est 0xabcd.
  - **size** *bytes* est la longueur du paquet envoyé. Par défaut, c'est de 100 octets.
  - **validate** indique que vous souhaitez valider les données de réponse.

- Ping TCP.

  ping tcp [*if_name*] *host* [*port*] [**repeat** *count*] [**timeout** *seconds*] [**source** *host* [*ports*]

  Lieu :

- *if_name* spécifie l'adresse IP source pour l'envoi d'un message Ping; cependant, l'interface de sortie est déterminée par une recherche de routage à l'aide de la table de routage des données.
- *host* est l'adresse IPv4 ou le nom d'hôte de la destination à laquelle vous envoyez un ping. Vous ne pouvez pas utiliser le Ping TCP avec les adresses IPv6.
- *port* est le port TCP de l'hôte auquel vous envoyez un message Ping.
- **repeat** et **timeout** ont la même signification que ci-dessus.
- **source** *host port* indique l'adresse IP source et le port pour envoyer un message Ping. Utilisez le port 0 pour obtenir un port aléatoire.

- Ping interactif.

  ping

  En saisissant un message Ping sans paramètres, vous êtes invité à indiquer l'interface, la destination et d'autres paramètres, y compris les paramètres étendus qui ne sont pas disponibles en tant que mots clés. Utilisez cette méthode si vous avez besoin d'un contrôle étendu sur les paquets Ping.

Tester la connectivité ASA de manière systématique

Si vous souhaitez effectuer un test plus systématique de la connectivité ASA, vous pouvez utiliser la procédure générale suivante.

Avant de commencer

Si vous souhaitez voir les messages de journal système mentionnés dans la procédure, activez la journalisation (la commande **logging enable**, ou **Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Setup (Configuration de la journalisation)** dans ASDM).

Bien que cela soit inutile, vous pouvez également activer le débogage ICMP pour afficher des messages sur la console ASA lorsque vous envoyez un message Ping aux interfaces ASA à partir de périphériques externes (vous ne verrez pas les messages de débogage pour les pings qui passent par l'ASA). Nous vous conseillons d'activer uniquement les messages Ping et de débogage pendant le dépannage, car ils peuvent affecter les performances. L'exemple suivant active le débogage ICMP, définit les messages de journal système à envoyer aux sessions Telnet ou SSH, les envoie à ces sessions et active la journalisation. Au lieu d'utiliser la commande **logging monitor debug**, vous pouvez également utiliser la commande **logging buffer debug** pour envoyer les messages du journal à un tampon, puis les afficher ultérieurement à l'aide de la commande **show logging**.

```
ciscoasa(config)# debug icmp trace
ciscoasa(config)# logging monitor debug
ciscoasa(config)# terminal monitor
ciscoasa(config)# logging enable
```

Avec cette configuration, vous obtiendrez un résultat similaire à celui-ci pour un ping réussi depuis un hôte externe (209.165.201.2) vers l'interface externe de l'ASA (209.165.201.1) :

```
ciscoasa(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
```

```
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

La sortie affiche la longueur du paquet ICMP (32 octets), l'identifiant de paquet ICMP (1) et le numéro de séquence ICMP (le numéro de séquence ICMP commence à 0 et est incrémenté chaque fois qu'une requête est envoyée).

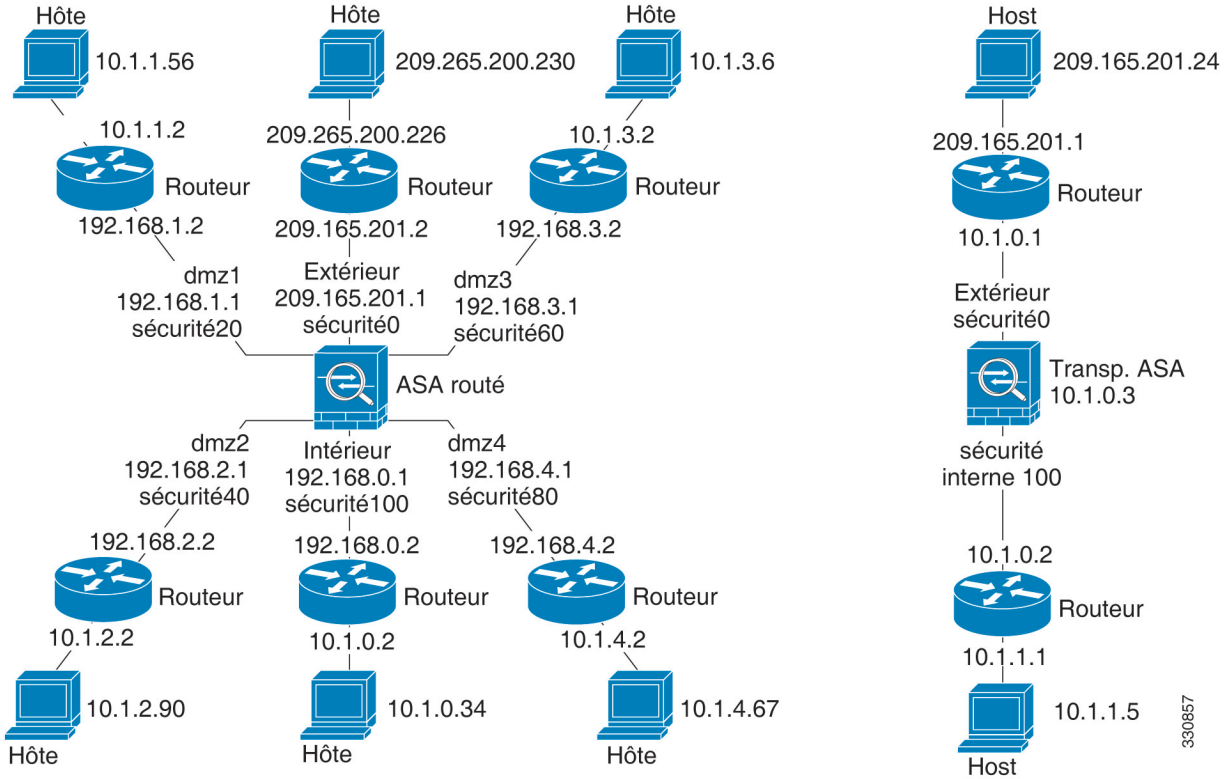
Lorsque vous avez terminé les tests, désactivez le débogage. Laisser la configuration en place peut présenter des risques de performance et de sécurité. Si vous avez activé la journalisation uniquement à des fins de test, vous pouvez également la désactiver.

```
ciscoasa(config)# no debug icmp trace
ciscoasa(config)# no logging monitor debug
ciscoasa(config)# no terminal monitor
ciscoasa(config)# no logging enable
```

Procédure

Étape 1 Tracez un diagramme de votre ASA ou de votre contexte de sécurité en mode unique qui affiche les noms d'interface, les niveaux de sécurité et les adresses IP. Le diagramme doit également inclure tous les routeurs directement connectés et un hôte de l'autre côté du routeur à partir duquel vous allez envoyer un message Ping à l'ASA.

Illustration 79 : Diagramme de réseau avec interfaces, routeurs et hôtes



Étape 2 Envoyez un ping à chaque interface ASA à partir des routeurs directement connectés. Pour le mode transparent, envoyez un message Ping à l'adresse IP des BVI. Ce test garantit que les interfaces ASA sont actives et que la configuration d'interface est correcte.

Un message Ping peut échouer si l'interface ASA n'est pas active, si la configuration d'interface est incorrecte ou si un commutateur entre l'ASA et un routeur est en panne (voir la figure suivante). Dans ce cas, aucun message de débogage ni message de journal système ne s'affiche, car le paquet n'atteint jamais l'ASA.

Illustration 80 : Échec de ping à l'interface ASA

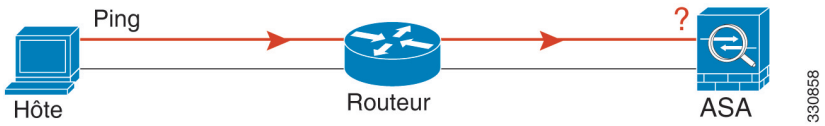
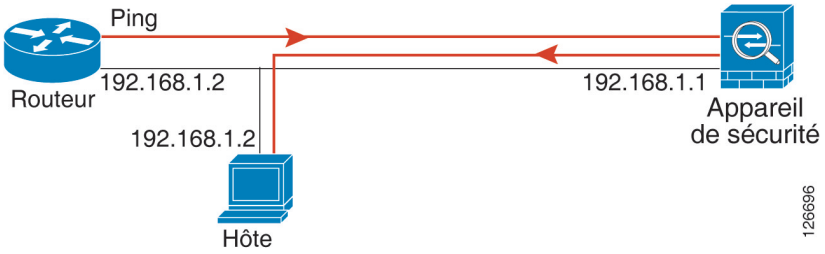


Illustration 81 : Échec de ping en raison de problèmes d'adressage IP



Si la réponse Ping ne revient pas au routeur, une boucle de commutation ou des adresses IP redondantes peuvent exister (voir la figure suivante).

Étape 3 Envoyez un ping à chaque interface ASA à partir d'un hôte distant. Pour le mode transparent, envoyez un message Ping à l'adresse IP des BVI. Ce test vérifie si le routeur connecté directement peut acheminer le paquet entre l'hôte et l'ASA et si l'ASA peut correctement acheminer le paquet vers l'hôte.

Un message Ping peut échouer si l'ASA n'a pas de route de retour vers l'hôte par le routeur intermédiaire (voir la figure suivante). Dans ce cas, les messages de débogage indiquent que l'envoi du message Ping a réussi, mais le message de journal système 110001 s'affiche, indiquant qu'une défaillance de routage s'est produite.

Illustration 82 : Échec de ping, car l'ASA n'a pas de route de retour



Étape 4 Envoyez un ping d'une interface ASA vers un périphérique réseau qui fonctionne correctement.

- Si le ping n'est pas reçu, il peut y avoir un problème avec le matériel de transmission ou la configuration de l'interface.
- Si l'interface ASA est configurée correctement et ne reçoit pas de réponse d'écho de l'appareil « connu pour être en bon état de fonctionnement », des problèmes avec la fonction de réception matérielle de l'interface peuvent exister. Si une interface différente ayant une capacité de réception « connue pour être bonne » peut recevoir un écho après avoir envoyé un message ping au même appareil « connu pour être bon », le problème de réception matérielle de la première interface est confirmé.

Étape 5 Envoyez un ping de l'hôte ou du routeur par l'interface source vers un autre hôte ou routeur sur une autre interface. Répétez cette étape pour autant de paires d'interfaces que vous souhaitez vérifier. Si vous utilisez la NAT, ce test montre que la NAT fonctionne correctement.

Si l'envoi d'un message Ping réussit, un message de journal système s'affiche pour confirmer la traduction d'adresses pour le mode routé (305009 ou 305011) et qu'une connexion ICMP a été établie (302020). Vous pouvez également saisir la commande **show xlate** ou **show conns** pour afficher ces renseignements.

L'envoi d'un message Ping peut échouer parce que la NAT n'est pas configurée correctement. Dans ce cas, un message de journal système s'affiche, indiquant que la NAT a échoué (305005 ou 305006). Si l'envoi d'un message Ping provient d'un hôte externe vers un hôte interne et que vous n'avez pas de traduction statique, vous recevez le message 106010.

Illustration 83 : Échec de ping parce que l'ASA ne traduit pas les adresses



Tracer les routes vers les hôtes

Si vous rencontrez des difficultés pour envoyer du trafic vers une adresse IP, vous pouvez tracer la route vers l'hôte pour déterminer s'il y a un problème sur le chemin réseau.

Procédure

Étape 1 Rendre l'ASA visible sur les routes de trace, à la page 1414.

Étape 2 Déterminer les routes de paquets, à la page 1416.

Rendre l'ASA visible sur les routes de trace

Par défaut, l'ASA n'apparaît pas sur les routes de trace en tant que saut. Pour l'afficher, vous devez décrémenter la durée de vie des paquets qui passent par l'ASA et augmenter la limite de débit pour les messages ICMP inaccessibles.

Procédure

Étape 1 Créez une carte de trafic L3/L4 pour identifier le trafic pour lequel vous souhaitez personnaliser les paramètres de connexion.

class-map *name*

match *parameter*

Exemple :

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
```

Pour en savoir plus sur les instructions correspondantes, consultez le chapitre Politique de service dans le guide de configuration du pare-feu.

Étape 2 Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

policy-map *name* **class** *name*

Exemple :

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
```

Dans la configuration par défaut, la liste des politiques global_policy est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste global_policy, saisissez global_policy comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

Étape 3 Décrémentez la durée de vie (TTL) sur les paquets correspondant à la classe.

```
set connection decrement-ttl
```

Étape 4 Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée global_policy), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

service-policy *policymap_name* {**global** | **interface** *interface_name* }

Exemple :

```
ciscoasa(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

Étape 5 Augmentez la limite de débit des messages ICMP inaccessibles afin que l'ASA s'affiche sur la sortie de la route de trace.

icmp unreachable rate-limit *rate* **burst-size** *size*

Exemple :

```
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 1
```

La limite de débit peut aller de 1 à 100, 1 étant la valeur par défaut. La taille de rafale n'a pas d'importance, mais doit être comprise entre 1 et 10.

Exemple

L'exemple suivant décrémente la TTL pour tout le trafic globalement et augmente la limite de messages ICMP inaccessibles à 50.

```
ciscoasa(config)# class-map global-policy
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class global-policy
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

Déterminer les routes de paquets

Utilisez la route de trace pour vous aider à déterminer la route que les paquets emprunteront pour atteindre leur destination. Une route de trace fonctionne en envoyant des paquets UDP ou des échos ICMPv6 à une destination sur un port non valide. Comme le port n'est pas valide, les routeurs situés sur le chemin vers la destination répondent par un message de dépassement de temps ICMP ou ICMPv6 et signalent cette erreur à l'ASA.

La route de trace affiche le résultat de chaque sonde envoyée. Chaque ligne de sortie correspond à une valeur TTL par ordre croissant. Le tableau suivant explique les symboles de sortie.

Symbole de sortie	Description
*	Aucune réponse n'a été reçue pour la sonde dans le délai d'expiration.
U	Aucune route vers la destination.
nn msec	Pour chaque nœud, le temps d'aller-retour (en millisecondes) pour le nombre spécifié de sondes.
!N.	Réseau ICMP inaccessible. Pour ICMPv6, l'adresse est hors du champ d'application.
!H	Hôte ICMP inaccessible.
!P	ICMP inaccessible. Pour ICMPv6, port inaccessible.
!A	ICMP administrativement interdit.
?	Erreur ICMP inconnue.

Procédure

Tracez la route vers une destination :

traceroute [*destination_ip* | *hostname*} [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

Exemple :

```
ciscoasa# traceroute 209.165.200.225

Type escape sequence to abort.
Tracing the route to 209.165.200.225

1 10.83.194.1 0 msec 10 msec 0 msec
2 10.83.193.65 0 msec 0 msec 0 msec
3 10.88.193.101 0 msec 10 msec 0 msec
4 10.88.193.97 0 msec 0 msec 10 msec
5 10.88.239.9 0 msec 10 msec 0 msec
6 10.88.238.65 10 msec 10 msec 0 msec
7 172.16.7.221 70 msec 70 msec 80 msec
8 209.165.200.225 70 msec 70 msec 70 msec

ciscoasa# traceroute 2002::130

Type escape sequence to abort.
Tracing the route to 2002::130

 1  5000::2 0 msec 0 msec 0 msec
 2  2002::130 10 msec 0 msec 0 msec
```

En règle générale, il suffit d'inclure l'adresse IP ou le nom d'hôte de destination, par exemple **traceroute www.example.com**. Cependant, vous pouvez ajuster les caractéristiques de la trace si vous le souhaitez :

- **source** {*source_ip* | *source-interface*} : spécifie l'interface à utiliser comme source de la trace. Vous pouvez définir l'interface par son nom ou par son adresse IP. Pour IPv6, vous ne pouvez pas spécifier l'interface source; vous pouvez uniquement spécifier l'adresse IP source. Une adresse IPv6 n'est valide que si vous avez activé IPv6 sur une interface ASA. En mode transparent, vous devez utiliser l'adresse de gestion.
- **numeric** : indique que seules les adresses IP doivent être affichées dans la route de trace. Sans ce mot clé, la route de trace effectue des recherches DNS pour les adresses et inclut les noms DNS, en supposant que vous configuriez le DNS.
- **timeout** *timeout_value* : durée d'attente d'une réponse avant l'expiration. La valeur par défaut est de 3 secondes.
- **probe** *probe_num* : nombre de sondes à envoyer à chaque niveau TTL. La valeur par défaut est de 3.
- **ttl** *min_ttl max_ttl* : valeurs de durée de vie minimum et maximum pour les sondes. La valeur minimum par défaut est de 1, mais vous pouvez la définir à une valeur plus élevée pour supprimer l'affichage des sauts connus. La valeur par défaut est 30. La route de trace se termine lorsque le paquet atteint sa destination ou lorsque la valeur maximum est atteinte.
- **port** *port_value* : le port UDP à utiliser. La valeur par défaut est 33434.
- **use-icmp** : envoie des paquets ICMP au lieu de paquets UDP pour les sondes.

Utiliser l'outil Packet Tracer pour tester la configuration de la politique

Vous pouvez tester la configuration de votre politique en modélisant un paquet basé sur des adresses source et de destination, et des caractéristiques de protocole. La trace effectue des recherches de politiques pour tester les critères d'accès, la NAT, le routage, etc., pour voir si le paquet est autorisé ou refusé.

En testant les paquets de cette manière, vous pouvez voir les résultats de vos politiques et vérifier si les types de trafic que vous souhaitez autoriser ou refuser sont gérés comme vous le souhaitez. En plus de vérifier votre configuration, vous pouvez utiliser le traceur pour déboguer un comportement inattendu, tel que le refus de paquets alors qu'ils devraient être autorisés.

Procédure

Étape 1 La commande est compliquée, nous l'avons donc divisée en parties. Commencez par choisir l'interface et le protocole de trace :

packet-tracer input *ifc_name* [**vlan-id***vlan_id*] {**icmp** | **tcp** | **udp** | **rawip** | **sctp**} [**inline-tag** *tag*] ...

Lieu :

- **input** *ifc_name* : nom de l'interface à partir de laquelle commencer la trace. Pour un groupe de ponts, spécifiez le nom de l'interface membre du groupe de ponts.
- **vlan-id** *vlan_id* : (Facultatif) Le LAN virtuel, où le traceur de paquets entre dans une interface parent, qui est ensuite redirigée vers une sous-interface. L'identité VLAN est disponible uniquement lorsque l'interface d'entrée n'est pas une sous-interface. Les valeurs valides sont comprises entre 1 et 4 096.
- **icmp**, **tcp**, **udp**, **rawip**, **sctp** : le protocole à utiliser. « rawip » désigne une adresse IP brute, c'est-à-dire des paquets IP qui ne sont pas TCP/ UDP.
- **inline-tag** *tag* : (Facultatif) La valeur de la balise du groupe de sécurité intégrée dans l'en-tête CMD de couche 2. Cette valeur peut être comprise entre 0 et 65 533.

Étape 2 Ensuite, saisissez l'adresse source et les critères de protocole.

...{*src_ip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}...

Lieu :

- *src_ip* : l'adresse IPv4 ou IPv6 source pour la trace de paquet.
- **user** *username* : l'identité de l'utilisateur au format domaine\utilisateur. L'adresse la plus récemment mappée pour l'utilisateur (le cas échéant) est utilisée dans la trace.
- **security-group** {**name** *name* | **tag** *tag*} : le groupe de sécurité source en fonction de la recherche IP-SGT de Trustsec. Vous pouvez spécifier un nom de groupe de sécurité ou un numéro de balise.
- **fqdn** *fqdn-string* : le nom de domaine complet de l'hôte source, IPv4 uniquement.

Étape 3 Ensuite, saisissez les caractéristiques du protocole.

- ICMP : saisissez le type ICMP (1 à 255), le code ICMP (0 à 255) et éventuellement l'identifiant ICMP. Vous devez utiliser des chiffres pour chaque variable, par exemple, 8 pour l'écho.

  type code... [*ident*]...

- TCP/UDP/SCTP : saisissez le numéro de port source.

  ...*src_port* ...

- Adresse IP brute : saisissez le numéro de protocole, de 0 à 255.

  … *protocol* ...

Étape 4 Enfin, saisissez les critères d'adresse de destination, le port de destination pour les traces TCP/UDP et les mots clés facultatifs, puis appuyez sur **Enter** (Entrée).

...dmac {*dst_ip* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *dst_port* [**detailed**] [**xml**]

Lieu :

- *dst_ip* : l'adresse IPv4 ou IPv6 de destination pour la trace de paquet.
- **security-group** {**name** *name* | **tag** *tag*} : le groupe de sécurité de destination en fonction de la recherche IP-SGT de Trustsec. Vous pouvez spécifier un nom de groupe de sécurité ou un numéro de balise.
- **fqdn** *fqdn-string* : le nom de domaine complet de l'hôte de destination, IPv4 uniquement.
- *dst_port* : le port de destination pour les traces TCP/UDP/SCTP. N'incluez pas cette valeur pour les traces ICMP ou IP brute.
- *dmac* : (Mode transparent) L'adresse MAC de destination.
- **detailed** : fournit des renseignements détaillés sur les résultats de la trace en plus de la sortie normale.
- **xml** : affiche les résultats de la trace au format XML.

Étape 5 Saisissez l'option **persist** pour que le traceur de paquets débogue les paquets sur les unités de grappe.

- Vous pouvez autoriser les paquets simulés à quitter l'ASA en utilisant l'option **transmit**.
- Pour ignorer les vérifications de sécurité comme les ACL, les filtres VPN, l'usurpation d'adresse IPsec et uRPF, utilisez l'option **bypass-checks**.
- En utilisant l'option **decrypted**, vous pouvez injecter un paquet déchiffré dans un tunnel VPN et simuler également un paquet qui traverse un tunnel VPN.

Étape 6 Saisissez l'**id** et l'**origin** pour suivre un paquet spécifique dans les unités de grappe.

- **id** : le numéro d'identité attribué par l'unité qui démarre la trace.
- **origin** : indique l'unité de grappe qui commence la trace.

Exemple

L'exemple suivant trace un paquet TCP pour le port HTTP de 10.100.10.10 à 10.100.11.11. Le résultat indique que le paquet sera abandonné par la règle implicite de refus d'accès.

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11
 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside

Phase: 2
```

```
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Supervision des connexions

Pour afficher les connexions actuelles avec des renseignements sur la source, la destination, le protocole, etc., utilisez la commande **show conn all detail**.

Historique des tests et du dépannage

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge IPv6 pour les routes de trace	9.7(1)	La commande **traceroute** a été modifiée pour accepter une adresse IPv6. Nous avons modifié la commande suivante : **traceroute**
Prise en charge de l'outil de trace de paquets pour les interfaces membres du groupe de ponts	9.7(1)	Vous pouvez désormais utiliser l'outil de trace de paquets pour les interfaces membres d'un groupe de ponts. Nous avons ajouté deux nouvelles options à la commande **packet-tracer**; **vlan-id** et **dmac**
Démarrer et arrêter manuellement les captures de paquets	9.7(1)	Vous pouvez maintenant arrêter et démarrer manuellement la capture. Commandes ajoutées ou modifiées : **capture stop**

Nom de la caractéristique	Versions de plateforme	Description
Capacités améliorées de l'outil de trace de paquets et de la capture de paquets	9.9(1)	L'outil de trace de paquets a été amélioré avec les fonctionnalités suivantes : • Tracer un paquet lorsqu'il passe entre les unités de grappe. • Autoriser des paquets simulés à quitter l'ASA. • Contourner les contrôles de sécurité pour un paquet simulé. • Considérer un paquet simulé comme un paquet IPsec/SSL déchiffré. La capture de paquets a été améliorée avec les fonctionnalités suivantes : • Capturer les paquets après leur déchiffrement. • Capturer les traces et les conserver dans la liste persistante. Commandes nouvelles ou modifiées : **cluster exec capture test trace include-decrypted, cluster exec capture test trace persist, cluster exec clear packet-tracer, cluster exec show packet-tracer id, cluster exec show packet-tracer origin, packet-tracer persist, packet-tracer transmit, packet-tracer decrypted, packet-tracer bypass-checks**
Prise en charge de la capture de paquets pour le trafic IPv6 correspondant sans l'utilisation d'une ACL	9.10(1)	Si vous utilisez le mot clé **match** pour la commande **capture**, le mot clé **any** ne correspond qu'au trafic IPv4. Vous pouvez désormais spécifier les mots clés **any4** et **any6** pour capturer le trafic IPv4 ou IPv6. Le mot clé **any** continue de correspondre uniquement au trafic IPv4. Commandes nouvelles ou modifiées : **capture match**

Nom de la caractéristique	Versions de plateforme	Description
Nouvelle commande **debug telemetry** pour Forepower 9300/4100.	9.14(1)	Si vous utilisez la commande **debug telemetry**, les messages de débogage liés à la télémétrie s'affichent. Les débogages aident à identifier la cause des erreurs lors de la génération du rapport de télémétrie. Commandes nouvelles ou modifiées : **[no] debug telemetry**,**show debug telemetry**
Modifications de la commande **ping**	9.18(2)	Pour prendre en charge l'envoi d'un message ping à une interface de boucle avec retour, la commande **ping** a maintenant changé de comportement. Si vous spécifiez l'interface dans la commande, l'adresse IP source correspond à l'adresse IP de l'interface spécifiée, mais l'interface de sortie réelle est déterminée par une recherche de route à l'aide de la table de routage des données. Commandes nouvelles ou modifiées : **ping**



PARTIE VIII

Surveillance

- Journalisation, à la page 1425
- MIB SNMP, à la page 1455
- Données de télémétrie et du Cisco Success Network, à la page 1495
- Alarmes pour Cisco ISA 3000, à la page 1507
- Rapports anonymes et Smart Call Home, à la page 1517



CHAPITRE 47

Journalisation

Ce chapitre décrit comment consigner les messages système et les utiliser pour la résolution de problèmes.

- À propos de la journalisation, à la page 1425
- Lignes directrices relatives à la journalisation, à la page 1433
- Configurer la journalisation, à la page 1435
- Supervision des journaux, à la page 1450
- Exemples de journalisation, à la page 1451
- Historique de journalisation, à la page 1452

À propos de la journalisation

La journalisation du système est une méthode de collecte de messages des périphériques vers un serveur exécutant un daemon syslog. La journalisation sur un serveur syslog central facilite l'agrégation des journaux et des alertes. Les périphériques Cisco peuvent envoyer leurs messages de journal à un service syslog de type UNIX. Un service syslog accepte les messages et les stocke dans des fichiers ou les imprimés conformément à un fichier de configuration simple. Cette forme de journalisation offre un stockage protégé à long terme pour les journaux. Les journaux sont utiles pour les dépannages de routine et pour le traitement des incidents.

Les journaux système d'ASA vous fournissent des renseignements pour superviser et dépanner l'ASA. La fonction de journalisation vous permet d'effectuer les opérations suivantes :

- Spécifier quels messages du journal système doivent être enregistrés.
- Désactiver ou modifier le niveau de gravité d'un message du journal système.
- Préciser au moins un emplacement où les messages du journal système doivent être envoyés, notamment :
  - Un tampon interne
  - Un ou plusieurs serveurs de journal système
  - ASDM
  - Une station de gestion SNMP
  - Des adresses courriel spécifiées
  - Console
  - Sessions Telnet et SSH.

- Configurer et gérer les messages de journal système en groupes, par exemple par niveau de gravité ou classe de message.
- Spécifier si une limite de débit est appliquée ou non à la génération du journal système.
- Préciser ce qu'il arrive au contenu du tampon du journal interne lorsqu'il est plein : écraser le tampon, envoyer le contenu du tampon à un serveur FTP ou enregistrer le contenu dans la mémoire flash interne.
- Filtrer les messages du journal système par emplacements, niveau de gravité, classe ou liste de messages sur mesure.

Journalisation dans le mode de contexte multiple

Chaque contexte de sécurité comprend sa propre configuration de journalisation et génère ses propres messages. Si vous vous connectez au contexte de système ou d'administration, puis passez à un autre contexte, les messages que vous affichez dans votre session ne sont que les messages liés au contexte actuel.

Les messages de journal système qui sont générés dans l'espace d'exécution du système, y compris les messages de basculement, sont consultés dans le contexte d'administration avec les messages générés dans le contexte d'administration. Vous ne pouvez pas configurer la journalisation ni afficher des renseignements de journalisation dans l'espace d'exécution du système.

Vous pouvez configurer l'ASA pour inclure le nom de contexte dans chaque message, ce qui vous aide à différencier les messages de contexte qui sont envoyés à un seul serveur de journal système. Cette fonctionnalité vous aide également à déterminer quels messages proviennent du contexte d'administration et lesquels proviennent du système. Les messages qui proviennent de l'espace d'exécution du système utilisent un ID de périphérique de **système**, et les messages qui proviennent du contexte d'administration utilisent le nom du contexte d'administration comme ID de périphérique.

Analyse des messages du journal système

Voici quelques exemples du type de renseignements que vous pouvez obtenir en examinant différents messages du journal système :

- Les connexions autorisées par les politiques de sécurité d'ASA. Ces messages vous aident à repérer les failles qui restent ouvertes dans vos politiques de sécurité.
- Les connexions refusées par les politiques de sécurité d'ASA. Ces messages indiquent quels types d'activités sont dirigées vers votre réseau interne sécurisé.
- L'utilisation de la fonctionnalité de journalisation du taux de refus ACE affiche les attaques qui se produisent sur votre ASA.
- Les messages d'activité d'IDS peuvent afficher les attaques qui se sont produites.
- L'authentification de l'utilisateur et l'utilisation des commandes fournissent une piste d'audit des modifications des politiques de sécurité.
- Les messages d'utilisation de la bande passante affichent chaque connexion qui a été établie et détruite, ainsi que la durée et le volume de trafic utilisés.
- Les messages d'utilisation des protocoles affichent les protocoles et les numéros de port utilisés pour chaque connexion.

- Les messages de piste d'audit de traduction d'adresses enregistrent les connexions NAT ou PAT en cours d'établissement ou de destruction, ce qui est utile si vous recevez un rapport des activités malveillantes provenant de l'intérieur de votre réseau vers l'extérieur.

Format des messages du journal système

Les messages du journal système sont structurés comme suit :

```
[<PRI>]: [Timestamp] [Device-ID] : %-Level-Message_number: Message_text
```

Les descriptions des champs sont les suivantes :

<PRI>	Valeur de la priorité. Lorsque la journalisation EMBLEM est activée, cette valeur s'affiche dans le message de journal système. La journalisation EMBLEM est compatible avec UDP et non avec TCP.
Horodatage	La date et l'heure de l'événement s'affichent. Lorsque la journalisation des horodatages est activée, et si l'horodatage est configuré pour être au format RFC 5424, tous les horodatages dans les messages de journal système affichent l'heure en heure UTC, comme indiqué par la norme RFC 5424.
Device-ID	La chaîne d'identifiant du périphérique qui a été configurée lors de l'activation de l'option logging device-id par l' interface utilisateur. Si cette option est activée, l'ID de périphérique n'apparaît pas dans les messages de journal système au format EMBLEM.
	Le code d'installation du message de journal système pour les messages générés par l'. Cette valeur est toujours .
Level (Niveau)	0 à 7. Le niveau reflète la gravité de la condition décrite par le message de journal système : plus le nombre est bas, plus la condition est critique.
Message_number	Un numéro à six chiffres unique qui identifie le message de journal système.
Message_text	Une chaîne de texte qui décrit la condition. Cette partie du message de journal système comprend parfois des adresses IP, des numéros de port ou des noms d'utilisateurs.

Tous les messages de journal système générés par le périphérique sont documentés dans le guide Messages de journal système de la série Cisco Secure Firewall ASA.

Le format syslog EMBLEM est une convention propre à Cisco, fondée sur les normes RFC 3164 et RFC 5424. Ainsi, lorsque EMBLEM est activé, le message syslog affiche deux-points (:) après le champ <PRI>.

Exemple de message de journal système avec la journalisation EMBLEM, la journalisation de l'horodatage RFC 5424 et l'ID de périphérique activés. Notez les deux-points (:) après le champ <PRI> (*<166>*).

```
<166>:2018-06-27T12:17:46Z: %-6-110002 : échec de localisation de l'interface de sortie
pour le protocole de l'interface src : port IP/src à l'adresse IP/au port de destination
```

Exemple de message de journal système avec la journalisation de l'horodatage RFC 5424 et l'ID de périphérique activés. Il n'y a pas de deux-points (:) avant l'horodatage.

```
2018-06-27T12:17:46Z  : %-6-110002 : échec de localisation de l'interface de sortie pour
le protocole de l'interface src : port IP/src à l'adresse IP/au port de destination
```

Niveaux de gravité

Le tableau suivant répertorie les niveaux de gravité des messages du journal système. Vous pouvez affecter des couleurs personnalisées à chacun des niveaux de gravité pour faciliter leur distinction dans les visualiseurs de journaux ASDM. Pour configurer les paramètres de couleur des messages du journal système, sélectionnez l'onglet **Outils > Préférences » Syslog** ou, dans la visionneuse de journal elle-même, cliquez sur **Paramètres de couleur** dans la barre d'outils.

Tableau 60 : Niveaux de gravité des messages Syslog

Numéro de niveau	Niveau de gravité	Description
0	**urgences**	Système inutilisable.
1	**alerte**	Action immédiate requise.
2	**critique**	Conditions critiques.
3	**erreur**	Conditions d'erreur.
4	**avertissement**	Conditions de mise en garde.
5	**notification**	Condition normale, mais pouvant être grave
6	**renseignements**	Messages informatifs seulement.
7	**débogage**	Messages de débogage uniquement Ne journalisez à ce niveau que temporairement, lors du débogage des problèmes. Ce niveau de journalisation peut générer tant de messages que les performances du système peuvent en être affectées.

Remarque ASA et ne génèrent pas de messages syslog avec un niveau de gravité de zéro (urgences).

Filtrage des messages Syslog

Vous pouvez filtrer les messages syslog générés de sorte que seuls certains messages syslog soient envoyés vers une destination de sortie particulière. Par exemple, vous pouvez configurer ASA pour envoyer tous les messages syslog vers une destination de sortie et pour envoyer un sous-ensemble de ces messages syslog vers une autre destination de sortie.

Plus précisément, vous pouvez diriger les messages du syslog vers une destination de sortie en fonction des critères suivants :

- Numéros d'ID des messages Syslog
- Niveau de gravité des messages du journal système
- Classe de messages Syslog (équivalente à une zone fonctionnelle)

Vous personnalisez ces critères en créant une liste de messages que vous pouvez préciser lorsque vous définissez la destination de sortie. Sinon, vous pouvez configurer les ASA pour envoyer une classe de messages particulière à chaque type de destination de sortie indépendamment de la liste de messages.

Classe de messages Syslog

Vous pouvez utiliser les classes de messages syslog de deux manières :

- Précisez un emplacement de sortie pour toute une catégorie de messages du journal système. Utilisez la commande **logging class**.
- Créez une liste de messages qui spécifie la classe du message. Utilisez la commande **logging list**.

La classe de messages syslog fournit une méthode de catégorisation des messages syslog par type, ce qui équivaut à une fonctionnalité ou à une fonction du périphérique. Par exemple, la classe rip désigne le routage RIP.

Tous les messages syslog d'une classe particulière partagent les trois mêmes chiffres initiaux dans leurs numéros d'ID de message syslog. Par exemple, tous les ID de message syslog qui commencent par les chiffres 611 sont associés à la classe vpnc (client VPN). Les messages syslog associés à la fonctionnalité de client VPN vont de 611101 à 611323.

En outre, la plupart des messages syslog ISAKMP ont un ensemble commun d'objets ajoutés au début pour aider à identifier le tunnel. Ces objets précèdent le texte descriptif d'un message syslog lorsqu'ils sont disponibles. Si l'objet est inconnu au moment de la génération du message syslog, la combinaison en-tête = valeur ne s'affiche pas.

Les objets portent le préfixe suivant :

Group = *groupname*, Username = *user*, IP = *IP_address*

Lorsque le groupe est le groupe de tunnels, le nom d'utilisateur est le nom d'utilisateur de la base de données locale ou du serveur AAA et l'adresse IP est l'adresse IP publique du client d'accès à distance ou de l'homologue de couche 2.

Le tableau suivant répertorie les classes de messages et la plage d'ID de message dans chaque classe.

Tableau 61 : Classes de messages syslog et numéros d'ID de messages associés

Classe	Définition	Numéros d'ID des messages Syslog
auth	Authentification de l'utilisateur	109, 113
—	Listes d'accès	106
—	Pare-feu d'application	415
—	Filtre de trafic de réseau de zombies	338
bridge (pont)	Pare-feu transparent	110, 220
ca	Autorité de certification de l'infrastructure de clé publique (PKI)	717
citrix	Client Citrix	723

Classe	Définition	Numéros d'ID des messages Syslog
—	Mise en grappe	747
—	Gestion des cartes	323
config (configurer)	Interface de commande	111, 112, 208, 308
csd	Poste de travail sécurisé	724
cts	TrustSec de Cisco	776
DAP	Politiques d'accès dynamique	734
eap, eapoudp	EAP ou EAPoUDP pour le contrôle d'admission au réseau	333, 334
eigrp	Routage EIGRP	336
e-mail	Serveur mandataire de courriel	719
—	Surveillance de l'environnement	735
ha	Basculement	101, 102, 103, 104, 105, 210, 311, 709
—	Pare-feu basé sur l'identité	746
ids	Système de détection des intrusions	400, 733
—	Boîte à outils IKEv2	750, 751, 752
ip	Pile d'adresse IP	209, 215, 313, 317, 408
ipaa	Affectation d'adresse IP	735
ips	Système de protection contre les intrusions	400, 401, 420
—	IPv6	325
—	Licence	444
mdm-proxy	Mandataire MDM	802.
nac	Contrôle d'admission au réseau (NAC)	731, 732
nacpolicy	Politique NAC	731
nacsettings	Paramètres NAC pour appliquer la politique NAC	732
—	NAT et PAT	305
—	Point d'accès réseau	713

Classe	Définition	Numéros d'ID des messages Syslog
np	Processeur de réseau	319
—	NP SSL	725
ospf	Routage OSPF	318, 409, 503, 613
—	Chiffrement de mot de passe	742
—	Serveur mandataire téléphonique	337
protocole RIP	Routage RIP	107, 312
rm	Gestionnaire des ressources	321
—	Smart Call Home	120
séance de formation	Séance d'utilisateur	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
snmp	SNMP	212
—	ScanSafe	775
ssl	Pile SSL	725
svc	Client VPN SSL	722
sys	Système	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	Détection des menaces	733
tag-switching	Commutation de balise de service	779
transactional-rule-engine-tre	Moteur de règles transactionnelles	780
uc-ims	UC-IMS	339
vm	Mise en correspondance VLAN	730
vpdn	Sessions PPTP et L2TP	213, 403, 603
vpn	IKE et IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	Client VPN	611
vpnfo	Basculement du VPN	720
vpnlb	Équilibrage de la charge VPN	718

Classe	Définition	Numéros d'ID des messages Syslog
—	VXLAN	778
webfo	Basculement WebVPN	721
webvpn	WebVPN et Secure Client (services client sécurisés)	716

Listes de messages personnalisés

La création d'une liste de messages personnalisée est un moyen flexible d'exercer un contrôle sur les messages du journal système qui sont envoyés vers une destination de sortie spécifique. Dans une liste de messages de journal système personnalisée, vous spécifiez des groupes de messages de journal système à l'aide d'un ou de tous les critères suivants :

- Niveau de gravité
- ID du message
- Plages d'ID des messages du journal système
- Classe de messages.

Par exemple, vous pouvez utiliser des listes de messages pour effectuer les opérations suivantes :

- Sélectionnez les messages du journal système avec les niveaux de gravité 1 et 2 et envoyez-les à une ou plusieurs adresses courriel.
- Sélectionnez tous les messages du journal système associés à une classe de messages (comme ha) et enregistrez-les dans le tampon interne.

Une liste de messages peut inclure plusieurs critères de sélection des messages. Cependant, vous devez ajouter chaque critère de sélection des messages à l'aide d'une nouvelle entrée de commande. Il est possible de créer une liste de messages qui comprend des critères de sélection des messages qui se chevauchent. Si deux critères d'une liste de messages sélectionnent le même message, le message est journalisé une seule fois.

Mise en grappe

Les messages du journal système sont un outil inestimable pour la comptabilité, la surveillance et le dépannage dans un environnement de grappe. Chaque unité ASA de la grappe (jusqu'à huit unités sont autorisées) génère des messages de journal système de manière indépendante; certaines commandes **logging** vous permettent ensuite de contrôler les champs d'en-tête, qui comprennent un horodatage et un ID de périphérique. Le serveur de journal système utilise l'ID de périphérique pour identifier le générateur de journaux systèmes. Vous pouvez utiliser la commande **logging device-id** pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant d'unités identiques ou différentes dans la grappe.

Lignes directrices relatives à la journalisation

Cette section comprend des consignes et des limites que vous devez consulter avant de configurer la journalisation.

Directives IPv6

- IPv6 est pris en charge. Les journaux système peuvent être envoyés en utilisant les protocoles TCP ou UDP.
- Assurez-vous que l'interface configurée pour l'envoi des journaux système est activée, qu'elle est compatible avec IPv6, et que le serveur syslog est accessible par l'intermédiaire de l'interface désignée.
- La journalisation sécurisée sur IPv6 n'est pas prise en charge.

Directives supplémentaires

- Le serveur syslog doit exécuter un programme de serveur appelé syslogd. Windows fournit un serveur syslog dans le cadre de son système d'exploitation.
- Le serveur syslog fonctionne selon le processus syslog-ng du système de pare-feu. N'utilisez pas de fichiers de configuration externes, comme le fichier *scwx.conf* de SecureWorks. Ces fichiers ne sont pas compatibles avec le périphérique. Leur utilisation entraînera une erreur d'analyse et, éventuellement, le processus syslog-ng échouera.
- Pour afficher les journaux générés par ASA, vous devez spécifier une destination de sortie de journalisation. Si vous activez la journalisation sans préciser de destination de sortie de journalisation, l'ASA génère des messages mais ne les enregistre pas à un emplacement à partir duquel vous pouvez les afficher. Vous devez spécifier chaque destination de sortie de journalisation séparément. Par exemple, pour désigner plusieurs serveurs syslog comme destination de sortie, saisissez une nouvelle commande pour chaque serveur syslog.
- L'envoi de journaux du système sur TCP n'est pas pris en charge sur un périphérique de secours.
- Si vous utilisez TCP comme protocole de transport, le système ouvre quatre connexions au serveur syslog pour s'assurer que les messages ne sont pas perdus. Si vous utilisez le serveur syslog pour collecter les messages d'un très grand nombre de périphériques et que le surdébit de la connexion combinée est trop important pour le serveur, utilisez plutôt UDP.
- Il n'est pas possible d'affecter deux listes ou classes différentes à des serveurs syslog différents ou aux mêmes emplacements.
- Vous pouvez configurer jusqu'à seize serveurs de journaux système. Cependant, en mode contexte multiple, la limitation est de 4 serveurs par contexte.
- Le serveur syslog doit être accessible au moyen de ASA. Vous devez configurer le périphérique pour refuser les messages ICMP unreachable (ICMP injoignable) sur l'interface par laquelle le serveur syslog est accessible et pour envoyer des journaux syslog au même serveur. Assurez-vous d'avoir activé la journalisation pour tous les niveaux de gravité. Pour éviter que le serveur syslog ne se bloque, supprimez la génération des syslogs 313001, 313004 et 313005.
- Le nombre de connexions UDP pour syslog est directement lié au nombre de CPU sur la plateforme matérielle et au nombre de serveurs syslog que vous configurez. À tout moment, il peut y avoir autant

de connexions syslog UDP qu'il y a de CPU multiplié par le nombre de serveurs syslog configurés. Il s'agit du comportement attendu. Notez que le délai d'inactivité de la connexion UDP globale s'applique à ces sessions et que la valeur par défaut est de 2 minutes. Vous pouvez ajuster ce paramètre si vous souhaitez fermer ces sessions plus rapidement, mais le délai d'expiration s'applique à toutes les connexions UDP, pas seulement au syslog.

- Lorsque vous utilisez une liste de messages personnalisée pour correspondre uniquement aux résultats de liste d'accès, les journaux de liste d'accès ne sont pas générés pour les listes dont le niveau de gravité de journalisation a été augmenté à débogage (niveau 7). Le niveau de gravité de la journalisation par défaut est défini à 6 pour la commande **logging list** (liste de journalisation). Ce comportement par défaut a été prévu. Lorsque vous modifiez explicitement le niveau de gravité de la journalisation de la configuration de la liste d'accès à Débogage, vous devez également modifier la configuration de journalisation elle-même.

  Voici un exemple de sortie de la commande **show running-config logging** qui n'inclut pas les résultats de la liste d'accès, car leur niveau de gravité de journalisation a été remplacé par « débogage » :

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging list test message 106100
  logging buffered test
  ```

  Voici un exemple de sortie de la commande **show running-config logging** qui n'inclut pas les résultats de la liste d'accès :

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging buffered debugging
  ```

  Dans ce cas, la configuration de la liste d'accès ne change pas et le nombre d'occurrences de la liste d'accès s'affiche, comme le montre l'exemple suivant :

  ```
  ciscoasa(config)# access-list global line 1 extended
  permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
  ciscoasa(config)# access-list global line 2 extended
  permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
  ciscoasa(config)# access-list global line 3 extended
  permit ip any any (hitcnt=543) 0x25f9e609
  ```

- Lorsque ASA envoie des journaux système via TCP, la connexion prend environ une minute pour s'établir après le redémarrage du service syslogd.
- Lorsque l'hôte de journalisation TCP tombe en panne, il faut environ 6 minutes pour faire passer son état de connexion de *Connected* (Connecté) à *Not connected* (Non connecté). La journalisation s'appuie sur le TCP pour détecter l'état du canal; jusqu'à ce moment-là, la journalisation envoie les journaux par le canal. Pendant ce temps, lorsque vous exécutez **show log**, la sortie affiche l'hôte de journalisation TCP comme connecté. Une fois que le canal TCP est fermé, l'état de l'hôte de journalisation TCP est mis à jour à *Not connected* (Non connecté).
- Le certificat de serveur reçu d'un serveur Syslog doit contenir « ServAuth » dans le champ Extended Key Usage (Utilisation de la clé étendue). Cette vérification sera effectuée uniquement pour les certificats non autosignés. Les certificats autosignés ne fournissent aucune valeur dans ce champ.

Configurer la journalisation

Cette section décrit comment configurer la journalisation.

Activer la journalisation

Pour activer la journalisation, procédez comme suit :

Procédure

Activer la journalisation

logging enable

Exemple :

```
ciscoasa(config)# logging enable
```

Configurer une destination de sortie

Pour optimiser l'utilisation des messages de journal système pour le dépannage et la surveillance des performances, nous vous conseillons de préciser un ou plusieurs emplacements où les messages de journal système doivent être envoyés, y compris un tampon de journal interne, un ou plusieurs serveurs de journal système externes, ASDM, une station de gestion SNMP, le port de console, des adresses courriel spécifiées ou des sessions Telnet et SSH.

Lorsque vous configurez la journalisation syslog sur une interface avec accès de gestion uniquement activé, les journaux liés au plan de données (ID du journal système 302015, 302014, 106023 et 304001) sont abandonnés et n'atteignent pas le serveur de journal système. Les messages du journal système sont abandonnés, car la table de routage du chemin d'accès ne dispose pas du routage de l'interface de gestion. Par conséquent, assurez-vous que l'interface que vous configurez dispose d'un accès de gestion uniquement désactivé.

Envoyer des messages du journal système à un serveur externe de journal système

Vous pouvez archiver les messages en fonction de l'espace disque disponible sur le serveur de journal système externe et manipuler les données de journalisation après leur enregistrement. Par exemple, vous pouvez préciser les actions à exécuter lorsque certains types de messages Syslog sont enregistrés, extraire les données du journal et enregistrer les enregistrements dans un autre fichier pour créer des rapports ou suivre les statistiques à l'aide d'un script spécifique au site.

Pour envoyer des messages de journal système à un serveur de journal système externe, procédez comme suit :

Procédure

Étape 1 Configurez l'ASA pour envoyer des messages aux serveurs de journal système.

Vous pouvez configurer l'ASA pour envoyer des messages aux serveurs de journal système IPv4 ou IPv6.

logging host *interface_name syslog_ip* [**tcp**[/*port*] | **udp** [/*port*] [**format emblem**]]

Exemple :

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp/1026
ciscoasa(config)# logging host dmz1 2002::1:1 udp/2020
```

Le mot clé **format emblem** active la journalisation au format EMBLEM pour le serveur de journal système avec UDP uniquement. L'argument *interface_name* spécifie l'interface par laquelle vous accédez au serveur de journal système. L'argument *syslog_ip* spécifie l'adresse IP du serveur de journal système. La paire mot clé-argument **tcp**[/*port*] ou **udp**[/*port*] spécifie que l'ASA doit utiliser TCP ou UDP pour envoyer des messages de journal système au serveur de journal système.

Vous pouvez configurer l'ASA pour envoyer des données à un serveur de journal système en utilisant UDP ou TCP, mais pas les deux. Le protocole par défaut est UDP si vous n'indiquez pas de protocole.

Avertissement
Si vous spécifiez TCP, lorsque l'ASA détecte les défaillances du serveur de journal système, pour des raisons de sécurité, les nouvelles connexions par l'ASA sont bloquées. Pour autoriser les nouvelles connexions, quelle que soit la connectivité à un serveur de journal système TCP, consultez l'étape 3.

Si vous spécifiez UDP, l'ASA continue d'autoriser les nouvelles connexions, que le serveur de journal système soit opérationnel ou non. Les valeurs de port valides sont comprises entre 1025 et 65535, pour l'un ou l'autre de ces protocoles. Le port UDP par défaut est 514. Le port TCP par défaut est 1470.

Étape 2 Spécifiez les messages de journal système qui doivent être envoyés au serveur de journal système.

logging trap {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging trap errors
```

Vous pouvez spécifier le numéro du niveau de gravité (1 à 7) ou le nom. Par exemple, si vous définissez le niveau de gravité 3, l'ASA envoie des messages de journal système pour les niveaux de gravité 3, 2 et 1. Vous pouvez spécifier une liste de messages sur mesure qui identifie les messages de journal système à envoyer au serveur de journal système.

Étape 3 (Facultatif) Désactivez la fonction pour bloquer les nouvelles connexions lorsqu'un serveur de journal système connecté au TCP est en panne.

logging permit-hostdown

Exemple :

```
ciscoasa(config)# logging permit-hostdown
```

Lorsque l'ASA est configuré pour envoyer des messages de journal système à un serveur de journal système basé sur TCP, et si le serveur de journal système est en panne ou la file d'attente du journal est pleine, les nouvelles connexions à l'ASA sont bloquées. Les nouvelles connexions sont à nouveau autorisées une fois que le serveur de journal système est de nouveau opérationnel et que la file d'attente du journal n'est plus pleine. À l'aide de cette commande, vous pouvez autoriser les nouvelles connexions même si le serveur de journal système n'est pas opérationnel.

Étape 4 (Facultatif) Définissez la fonction de journalisation sur une valeur autre que 20, qui est celle attendue par la plupart des systèmes UNIX.

logging facility *number*

Exemple :

```
ciscoasa(config)# logging facility 21
```

Activer la journalisation sécurisée

Procédure

Activez la journalisation sécurisée en spécifiant le mot clé **secure** dans la commande de l'hôte de journalisation. En outre, saisissez éventuellement la commande **reference-identity**.

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**[**reference-identity** *reference_identity_name*]]

Lieu :

- **logging host** *interface_name syslog_ip* spécifie l'interface sur laquelle se trouve le serveur de journal système et l'adresse IP du serveur de journal système.
- [**tcp**/*port* | **udp**/*port*] spécifie le port (TCP ou UDP) que le serveur de journal système écoute pour les messages du journal système. Le mot clé **tcp** indique que l'ASA doit utiliser TCP pour envoyer des messages du journal système au serveur de journal système. Le mot clé **udp** indique que l'ASA doit utiliser UDP pour envoyer des messages du journal système au serveur de journal système.
- Le mot clé **format emblem** active la journalisation au format EMBLEM pour le serveur de journal système.
- Le mot clé **secure** indique que la connexion à l'hôte de journalisation distant doit utiliser SSL/TLS pour TCP uniquement. La journalisation sécurisée ne prend pas en charge UDP; une erreur se produit si vous essayez d'utiliser ce protocole.
- [**reference-identity** *reference_identity_name*] active les vérifications d'identité de référence RFC 6125 sur le certificat en fonction de l'objet d'identité de référence précédemment configuré. Consultez Configurer les identités de référence, à la page 910 pour en savoir plus sur l'objet d'identité de référence.

Exemple :

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure  reference-identity
syslogServer
```

Générer des messages du journal système en format EMBLEM vers un serveur de journal système

Pour générer des messages de journal système au format EMBLEM vers un serveur de journal système, procédez comme suit :

Procédure

Envoyez des messages de journal système au format EMBLEM à un serveur de journal système sur UDP en utilisant le port 514.

logging host *interface_name ip_address*{**tcp** [/*port*] | **udp** [/ *port*]] [**format emblem**]

Exemple :

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
ciscoasa(config)# logging host interface_1 2001::1 udp format emblem
```

Vous pouvez configurer des serveurs de journal système IPv4 ou IPv6.

Le mot clé **format emblem** active la journalisation au format EMBLEM pour le serveur de journal système (UDP uniquement). L'argument *interface_name* spécifie l'interface par laquelle vous accédez au serveur de journal système. L'argument *ip_address* spécifie l'adresse IP du serveur de journal système. La paire mot clé-argument **tcp**[/*port*] or **udp**[/*port*] spécifie que l'ASA doit utiliser TCP ou UDP pour envoyer des messages de journal système au serveur de journal système.

Vous pouvez configurer l'ASA pour envoyer des données à un serveur de journal système en utilisant UDP ou TCP. Le protocole par défaut est UDP si vous n'indiquez pas de protocole.

Vous pouvez utiliser plusieurs commandes **logging host** pour spécifier des serveurs supplémentaires qui recevront tous des messages de journal système. Si vous configurez au moins deux serveurs de journalisation, veillez à limiter le niveau de gravité de la journalisation aux avertissements pour tous les serveurs de journalisation.

Avertissement
Si vous spécifiez TCP, lorsque l'ASA détecte les défaillances du serveur de journal système, pour des raisons de sécurité, les nouvelles connexions par l'ASA sont bloquées. Pour autoriser de nouvelles connexions malgré les défaillances du serveur de journal système, consultez l'étape 3 de Envoyer des messages du journal système à un serveur externe de journal système, à la page 1435.

Si vous spécifiez UDP, l'ASA continue d'autoriser les nouvelles connexions, que le serveur de journal système soit opérationnel ou non. Les valeurs de port valides sont comprises entre 1025 et 65535, pour l'un ou l'autre de ces protocoles. Le port UDP par défaut est 514. Le port TCP par défaut est 1470.

Remarque
L'envoi de journaux système sur TCP n'est pas pris en charge sur un ASA de secours.

Générer des messages du journal système en format EMBLEM vers d'autres destinations de sortie

Pour générer des messages de journal système au format EMBLEM vers d'autres destinations de sortie, procédez comme suit :

Procédure

Envoyez des messages de journal système au format EMBLEM à des destinations de sortie autres qu'un serveur de journal système, comme des sessions Telnet ou SSH.

logging emblem

Exemple :

```
ciscoasa(config)# logging emblem
```

Envoyer les messages du journal système au tampon du journal interne

Vous devez spécifier quels messages de journal système doivent être envoyés au tampon du journal interne, qui sert d'emplacement de stockage temporaire. Les nouveaux messages sont ajoutés à la fin de la liste. Lorsque le tampon est plein, c'est-à-dire lorsqu'il arrive à saturation, les anciens messages sont remplacés par de nouveaux messages, sauf si vous configurez l'ASA pour enregistrer le tampon complet à un autre emplacement.

Pour envoyer des messages de journal système au tampon du journal interne, procédez comme suit :

Procédure

Étape 1 Spécifiez quels messages de journal système doivent être envoyés au tampon du journal interne, qui sert d'emplacement de stockage temporaire.

logging buffered {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging buffered critical
ciscoasa(config)# logging buffered level 2
ciscoasa(config)# logging buffered notif-list
```

Les nouveaux messages sont ajoutés à la fin de la liste. Lorsque le tampon est plein, c'est-à-dire lorsqu'il arrive à saturation, les anciens messages sont remplacés par de nouveaux messages, sauf si vous configurez l'ASA pour enregistrer le tampon complet à un autre emplacement. Pour vider le tampon du journal interne, saisissez la commande **clear logging buffer**.

Étape 2 Modifiez la taille du tampon du journal interne. La taille du tampon par défaut est de 4 Ko.

logging buffer-size *bytes*

Exemple :

```
ciscoasa(config)# logging buffer-size 16384
```

Remarque

Lorsque vous modifiez la taille du tampon de journalisation, les journaux existants dans le tampon sont purgés et un nouveau tampon est créé avec la taille nouvellement configurée.

Étape 3 Choisissez une des options suivantes :

- Enregistrez les nouveaux messages dans le tampon du journal interne et enregistrez le contenu complet de ce tampon dans la mémoire flash interne.

  logging flash-bufferwrap

  Exemple :

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

  Remarque
  Si la taille de tampon est supérieure à 2 Mo, cette commande arrête d'écrire des données dans la mémoire flash, sans avertissement.

- Enregistrez les nouveaux messages dans le tampon du journal interne et enregistrez le contenu complet du tampon du journal sur un serveur FTP.

  logging ftp-bufferwrap

  Exemple :

  ```
  ciscoasa(config)# logging ftp-bufferwrap
  ```

  Lors de l'enregistrement du contenu du tampon à un autre emplacement, l'ASA crée des fichiers journaux avec des noms qui utilisent le format d'horodatage suivant :

  ```
  LOG-YYYY-MM-DD-HHMMSS.TXT
  ```

  où *AAAA* est l'année, *MM* est le mois, *JJ* est le jour du mois et *HHMMSS* est la durée en heures, minutes et secondes.

- Identifiez le serveur FTP sur lequel vous souhaitez stocker le contenu du tampon du journal.

  logging ftp-server *server pathusername password*

  Exemple :

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

  L'argument *server* spécifie l'adresse IP du serveur FTP externe. L'argument *path* spécifie le chemin d'accès au répertoire sur le serveur FTP où les données du tampon du journal doivent être enregistrées. Ce chemin est relatif au répertoire racine FTP. L'argument *username* spécifie un nom d'utilisateur valide pour la connexion au serveur FTP. L'argument *password* indique le mot de passe pour le nom d'utilisateur spécifié.

- Enregistrez le contenu actuel du tampon du journal dans la mémoire flash interne.

  logging savelog [*savefile*]

  Exemple :

```
ciscoasa(config)# logging savelog latest-logfile.txt
```

Modifier la quantité de mémoire flash interne disponible pour les journaux

Pour modifier la quantité de mémoire flash interne disponible pour les journaux, procédez comme suit :

Procédure

Étape 1 Spécifiez la quantité maximum de mémoire flash interne disponible pour l'enregistrement des fichiers journaux.

logging flash-maximum-allocation *kbytes*

Exemple :

```
ciscoasa(config)# logging flash-maximum-allocation 1200
```

Par défaut, l'ASA peut utiliser jusqu'à 50 Mo de mémoire flash interne pour les données des journaux. La quantité minimum de mémoire flash interne qui doit être libre pour que l'ASA enregistre les données du journal est de 3 Mo. La limite maximum de la valeur flash-maximum-allocation est de 2 Go.

Si un fichier journal enregistré dans la mémoire flash interne entraîne une diminution de l'espace libre dans la mémoire flash interne en dessous de la limite minimum configurée, l'ASA supprime les fichiers journaux les plus anciens afin de garantir qu'il reste suffisamment d'espace libre après l'enregistrement du nouveau fichier journal. S'il n'y a aucun fichier à supprimer ou si, après la suppression de tous les anciens fichiers, la mémoire libre reste inférieure à la limite, l'ASA ne parvient pas à enregistrer le nouveau fichier journal.

Étape 2 Spécifiez la quantité minimum de mémoire flash interne qui doit être libre pour que l'ASA enregistre un fichier journal.

logging flash-minimum-free *kbytes*

Exemple :

```
ciscoasa(config)# logging flash-minimum-free 4000
```

Envoyer des messages Syslog à une adresse courriel

Pour envoyer des messages de journal système à une adresse courriel, procédez comme suit :

Procédure

Étape 1 Spécifiez quels messages de journal système doivent être envoyés à une adresse courriel.

logging mail {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging mail high-priority
```

Lors de l'envoi par courriel, un message de journal système s'affiche dans la ligne d'objet du courriel. Pour cette raison, nous vous conseillons de configurer cette option pour informer les administrateurs des messages de journal système de niveau de gravité élevé, tels que critique, alerte et urgence.

Étape 2 Spécifiez l'adresse courriel source à utiliser lors de l'envoi des messages de journal système à une adresse courriel.

logging from-address *email_address*

Exemple :

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

Étape 3 Spécifiez l'adresse courriel du destinataire à utiliser lors de l'envoi des messages de journal système à une adresse courriel.

logging recipient-address *e-mail_address*[*severity_level*]

Exemple :

```
ciscoasa(config)# logging recipient-address admin@example.com
```

Étape 4 Spécifiez le serveur SMTP à utiliser lors de l'envoi des messages de journal système à une adresse courriel. Vous pouvez fournir une adresse de serveur principal et secondaire pour assurer le service de messagerie du journal sans défaillance. Vous pouvez également associer une interface et le serveur pour identifier la table de routage à utiliser pour la journalisation. Si aucune interface n'est fournie, l'ASA fera référence à la table de routage de gestion et, en l'absence d'entrée de route, il examinera la table de routage des données.

smtp-server [*primary-interface*] *primary-smpt-server-ip-address* [[*backup-interface*]*backup-smpt-server-ip-address*]

Exemple :

```
ciscoasa(config)# smtp-server 10.1.1.24 10.1.1.34
ciscoasa(config)# smtp-server 10.1.1.24
ciscoasa(config)# smtp-server management 10.1.1.24 outside 10.1.1.34
ciscoasa(config)# smtp-server management 10.1.1.24
```

Envoyer les messages du journal système au gestionnaire ASDM

Pour envoyer des messages de journal système à ASDM, procédez comme suit :

Procédure

Étape 1 Spécifiez les messages de journal système qui doivent être envoyés à ASDM.

logging asdm {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging asdm 2
```

L'ASA réserve une zone de tampon pour les messages de journal système en attente d'envoi à ASDM et enregistre les messages dans le tampon au fur et à mesure qu'ils apparaissent. Le tampon du journal ASDM est un tampon différent de celui du tampon interne. Lorsque le tampon du journal ASDM est plein, l'ASA supprime le message de journal système le plus ancien afin de libérer de l'espace dans le tampon pour les nouveaux messages. La suppression du message de journal système le plus ancien pour faire de la place aux nouveaux messages est le paramètre par défaut dans ASDM. Pour contrôler le nombre de messages de journal système conservés dans le tampon du journal ASDM, vous pouvez modifier la taille de ce tampon.

Étape 2 Spécifiez le nombre de messages de journal système à conserver dans le tampon du journal ASDM.

logging asdm-buffer-size *num_of_msgs*

Exemple :

```
ciscoasa(config)# logging asdm-buffer-size 200
```

Saisissez la commande **clear logging asdm** pour vider le contenu actuel du tampon du journal ASDM.

Configurer la file d'attente de journalisation

Pour configurer la file d'attente de journalisation, procédez comme suit :

Procédure

Spécifiez le nombre de messages de journal système que l'ASA peut contenir dans sa file d'attente avant de les envoyer à la destination de sortie configurée.

logging queue *message_count*

Exemple :

```
ciscoasa(config)# logging queue 300
```

Les ASA ont un nombre fixe de blocs en mémoire qui peuvent être alloués pour la mise en mémoire tampon des messages du journal système en attente d'envoi à la destination de sortie configurée. Le nombre de blocs requis dépend de la longueur de la file d'attente des messages de journal système et du nombre de serveurs de journal système spécifié. La taille de la file d'attente par défaut est de 512 messages de journal système. La taille de la file d'attente n'est limitée que par la disponibilité de la mémoire de blocage. Les valeurs valides vont de 0 à 8 192 messages, selon la plateforme. Si la file d'attente de journalisation est fixée à zéro, la file d'attente a la taille configurable maximale (8 192 messages).

Envoyer les messages du journal système au port de console

Pour envoyer des messages de journal système au port de console, procédez comme suit :

Procédure

Spécifiez quels messages de journal système doivent être envoyés au port de console.

logging console { *severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging console errors
```

Envoyer les messages du journal système au serveur SNMP

Pour activer la journalisation sur un serveur SNMP, procédez comme suit.

Procédure

Activez la journalisation SNMP et spécifiez les messages à envoyer aux serveurs SNMP.

logging history [*logging_list* | *level*]

Exemple :

```
ciscoasa(config)# logging history errors
```

Envoyer les messages du journal système à une session Telnet ou SSH

Pour envoyer des messages de journal système à une session Telnet ou SSH, procédez comme suit :

Procédure

Étape 1 Spécifiez quels messages de journal système doivent être envoyés à une session Telnet ou SSH.

logging monitor {*severity_level* | *message_list*}

Exemple :

```
ciscoasa(config)# logging monitor 6
```

Étape 2 Activez la journalisation pour la session en cours uniquement.

terminal monitor

Exemple :

```
ciscoasa(config)# terminal monitor
```

Si vous vous déconnectez puis vous reconnectez, vous devrez saisir à nouveau cette commande. Saisissez la commande **terminal no monitor** pour désactiver la journalisation pour la session en cours.

Configurer les messages du journal système

Afficher ou masquer les noms d'utilisateur non valides dans les journaux système

Vous pouvez afficher ou masquer les noms d'utilisateur non valides dans les messages du journal système en cas de tentatives de connexion infructueuses. Le paramètre par défaut consiste à masquer les noms d'utilisateur lorsque le nom d'utilisateur est non valide ou si la validité est inconnue. Si un utilisateur saisit accidentellement un mot de passe au lieu d'un nom d'utilisateur, par exemple, il est plus sûr de masquer le « nom d'utilisateur » dans le message du journal système résultant. Vous souhaiterez peut-être afficher les noms d'utilisateur non valides pour résoudre les problèmes de connexion.

Procédure

Étape 1 Afficher les noms d'utilisateur non valides :

no logging hide username

Étape 2 Masquer les noms d'utilisateur non valides :

logging hide username

Inclure la date et l'heure dans les messages du journal système

Pour inclure la date et l'heure dans les messages du journal système, procédez comme suit :

Procédure

Précisez que les messages du journal système doivent inclure la date et l'heure auxquelles ils ont été générés.

logging timestamp

Exemple :

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

Pour supprimer la date et l'heure des messages du journal système, saisissez la commande **no logging timestamp**.

Désactiver un message du journal système

Pour désactiver un message du journal système spécifié, procédez comme suit :

Procédure

Empêchez l'ASA de générer un message de journal système particulier.

no logging message *syslog_id*

Exemple :

```
ciscoasa(config)# no logging message 113019
```

Pour réactiver un message du journal système désactivé, saisissez la commande **logging message** *syslog_id* (par exemple, **logging message 113019**). Pour réactiver la journalisation de tous les messages du journal système désactivés, saisissez la commande **clear configure logging disabled**.

Modifier le niveau de gravité d'un message du journal système

Pour modifier le niveau de gravité d'un message du journal système, procédez comme suit :

Procédure

Spécifiez le niveau de gravité d'un message du journal système.

logging message *syslog_id* **level** *severity_level*

Exemple :

```
ciscoasa(config)# logging message 113019 level 5
```

Pour réinitialiser le niveau de gravité d'un message du journal système à ses paramètres, saisissez la commande **no logging message** *syslog_id* **level** *severity_level* (par exemple, **no logging message 113019 level 5**). Pour réinitialiser le niveau de gravité de tous les messages du journal système modifiés à leurs paramètres, saisissez la commande **clear configure logging level**.

Bloquer les messages du journal système sur une unité de secours

Procédure

Utilisez la commande suivante pour bloquer la génération d'un message de journal système spécifique sur une unité de secours.

no logging message *syslog-id* **standby**

Exemple :

```
ciscoasa(config)# no logging message 403503 standby
```

Débloquez un message du journal système donné pour vous assurer que les messages de journal système de l'ASA de secours pour le basculement restent synchronisés si le basculement se produit. Utilisez la commande **logging standby** pour débloquer la génération d'un message de journal système spécifique qui a précédemment été bloqué et ne peut pas être généré sur une unité de secours.

Remarque
Dans un état stable, lorsque les ASA actifs et en veille enregistrent les journaux, le trafic double sur les destinations de journalisation partagées, telles que les serveurs de journal système, les serveurs SNMP et les serveurs FTP. Cependant, en cas de basculement, pendant la phase de commutation, l'ASA de secours génère plus d'événements, y compris les intrusions de basculement et les événements de connexion de l'unité active.

Inclure l'ID de périphérique dans les messages du journal système au format non EMBLEM

Pour inclure l'ID de périphérique dans les messages du journal système au format non EMBLEM, procédez comme suit :

Procédure

Configurez l'ASA pour inclure un ID de périphérique dans les messages du journal système au format non EMBLEM. Vous ne pouvez spécifier qu'un seul type d'ID de périphérique pour les messages du journal système.

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

Exemple :

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# logging device-id context-name
```

Le mot clé **context-name** indique que le nom du contexte actuel doit être utilisé comme ID de périphérique (s'applique au mode de contexte multiple uniquement). Si vous activez l'ID de périphérique de journalisation pour le contexte d'administration en mode de contexte multiple, les messages provenant de l'espace d'exécution du système utilisent un ID de périphérique de **system** et les messages provenant du contexte d'administration utilisent le nom du contexte d'administration comme ID de périphérique.

Remarque
Dans une grappe ASA, utilisez toujours l'adresse IP de l'unité de contrôle pour l'interface sélectionnée.

Le mot clé **cluster-id** spécifie le nom unique dans la configuration de démarrage d'une unité ASA individuelle dans la grappe en tant qu'ID de périphérique. Le mot clé **hostname** spécifie que le nom d'hôte de l'ASA doit être utilisé comme ID de périphérique. La paire mot clé-argument **ipaddress** *interface_name* précise que l'adresse IP de l'interface spécifiée comme *interface_name* doit être utilisée comme ID de périphérique. Si vous utilisez le mot clé **ipaddress**, l'ID de périphérique devient l'adresse IP de l'interface ASA spécifiée, quelle que soit l'interface à partir de laquelle le message de journal système est envoyé. Dans l'environnement de grappe, le mot clé **system** détermine que l'ID de périphérique devient l'adresse IP système sur l'interface. Ce mot clé fournit un ID de périphérique unique et cohérent pour tous les messages de journal système envoyés à partir du périphérique. La paire mot clé-argument **string** *text* spécifie que la chaîne de texte doit être utilisée comme ID de périphérique. La chaîne peut inclure jusqu'à 16 caractères.

Vous ne pouvez pas utiliser d'espaces ni l'un des caractères suivants :

- & (esperluette)
- ‘ (guillemets simples)
- “ (guillemets doubles)
- < (inférieur à)
- > (supérieur à)
- ? (point d'interrogation)

Remarque
Si cette option est activée, l'ID de périphérique n'apparaît pas dans les messages de journal système au format EMBLEM ni dans les alertes SNMP.

Créer une liste d'événements personnalisée

Vous utilisez les trois critères suivants pour définir une liste d'événements :

- Classe d'événement
- Gravité
- ID du message

Pour créer une liste d'événements personnalisées à envoyer à une destination de journalisation spécifique (par exemple, un serveur SNMP), procédez comme suit :

Procédure

Étape 1 Spécifiez les critères de sélection des messages à enregistrer dans le tampon du journal interne. Par exemple, si vous définissez le niveau de gravité 3, l'ASA envoie des messages de journal système pour les niveaux de gravité 3, 2 et 1.

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

Exemple :

```
ciscoasa(config)# logging list list-notif level 3
```

L'argument *name* spécifie le nom de la liste. La paire mot clé-argument **level** *level* spécifie le niveau de gravité. La paire mot clé-argument **class** *message_class* spécifie une classe de messages particulière. La paire mot clé-argument **message** *start_id* [*-end_id*] spécifie un numéro de message de journal système individuel ou une plage de numéros.

Remarque
N'utilisez pas les noms des niveaux de gravité comme nom d'une liste de messages de journal système. Les noms interdits comprennent les urgences, les alertes, les critiques, les erreurs, les avertissements, les notifications, les renseignements et le débogage. De même, n'utilisez pas les trois premiers caractères de ces mots au début d'un nom de liste d'événements. Par exemple, n'utilisez pas un nom de liste d'événements commençant par le caractère « err ».

Étape 2 (Facultatif) Ajoutez d'autres critères de sélection des messages à la liste.

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

Exemple :

```
ciscoasa(config)# logging list list-notif message 104024-105999
ciscoasa(config)# logging list list-notif level critical
ciscoasa(config)# logging list list-notif level warning class ha
```

Saisissez la même commande qu'à l'étape précédente, en précisant le nom de la liste de messages existante et le critère supplémentaire. Saisissez une nouvelle commande pour chaque critère que vous souhaitez ajouter à la liste. Par exemple, vous pouvez spécifier les critères pour les messages de journal système à inclure dans la liste comme suit :

- ID des messages du journal système compris entre 104 024 et 105 999.
- Tous les messages du journal système de niveau de gravité Critique ou supérieur (urgence, alerte ou critique).
- Tous les messages du journal système de classe ha avec un niveau de gravité d'avertissement ou supérieur (urgence, alerte, critique, erreur ou avertissement).

Remarque
Un message de journal système est journalisé s'il satisfait à l'une de ces conditions. Si un message de journal système satisfait à plusieurs conditions, le message est journalisé une seule fois.

Configurer les filtres de journalisation

Envoyer tous les messages du journal système d'une classe vers une destination de sortie spécifiée

Pour envoyer tous les messages du journal système d'une classe vers une destination de sortie spécifiée, procédez comme suit :

Procédure

Remplacez la configuration dans la commande de destination de sortie indiquée. Par exemple, si vous précisez que les messages de niveau de gravité 7 doivent être envoyés au tampon de journal interne et que les messages de classe ha de niveau de gravité 3 doivent être envoyés au tampon de journal interne, la dernière configuration prévaut.

logging class *message_class* {**buffered** | **console** | **history** | **mail** | **monitor** | **trap**} [*severity_level*]

Exemple :

```
ciscoasa(config)# logging class ha buffered alerts
```

Les mots clés **buffered**, **history**, **mail**, **monitor** et **trap** spécifient la destination de sortie à laquelle les messages du journal système de cette classe doivent être envoyés. Le mot clé **history** active la journalisation SNMP. Le mot clé **monitor** active la journalisation Telnet et SSH. Le mot clé **trap** active la journalisation du serveur de journal système. Sélectionnez une destination par entrée de ligne de commande. Pour spécifier qu'une classe doit être envoyée à plusieurs destinations, saisissez une nouvelle commande pour chaque destination de sortie.

Limiter le débit de génération des messages Syslog

Pour limiter le débit de génération des messages du journal système, procédez comme suit :

Procédure

Appliquez un niveau de gravité spécifié (1 à 7) à un ensemble de messages ou à un message en particulier (et non à la destination) dans une période donnée.

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

Exemple :

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

Les limites de débit ont une incidence sur le volume de messages envoyés à toutes les destinations configurées. Pour réinitialiser la limite de débit de journalisation à la valeur par défaut, saisissez la commande **clear running-config logging rate-limit**. Pour réinitialiser la limite de débit de journalisation, saisissez la commande **clear configure logging rate-limit**.

Supervision des journaux

Consultez les commandes suivantes pour superviser l'état de la journalisation.

- **show logging**

  Cette commande affiche les messages du journal système, y compris le niveau de gravité.

Remarque

- Le nombre maximum de messages de journal système pouvant être affichés est de 1 000, ce qui correspond au paramètre par défaut. Le nombre maximum de messages de journal système pouvant être affichés est de 2 000.
- Le compteur Host TX dans la sortie de la commande **show logging** s'affiche même après l'exécution de la commande **clear logging counters all**.

- **show logging message**

  Cette commande affiche une liste des messages de journal système avec les niveaux de gravité modifiés et des messages de journal système désactivés.

- **show logging message** *message_ID*

  Cette commande affiche le niveau de gravité d'un message de journal système spécifique.

- **show logging queue**

  Cette commande affiche la file d'attente de journalisation et les statistiques de la file d'attente.

- **show running-config logging rate-limit**

  Cette commande affiche le paramètre de limite de débit de journalisation actuel.

- **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Critères d'accès)**

  Ce volet vous permet de filtrer la visionneuse en direct de la journalisation de ces journaux en fonction des critères de recherche (ID hexadécimal de la règle). Pour afficher les résultats, sélectionnez la règle et cliquez sur **Show Log** (Afficher le journal).

Exemples de journalisation

Les exemples suivants montrent les renseignements de journalisation qui s'affichent pour la commande **show logging** :

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

```
ciscoasa (config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: enabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 330272 messages logged
    Trap logging: level debugging, facility 20, 325464 messages logged
        Logging to inside 2001:164:5:1::123
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

Les exemples suivants montrent comment contrôler l'activation d'un message de journal système et le niveau de gravité du message de journal système spécifié :

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

Historique de journalisation

Tableau 62 : Historique de journalisation

Nom de la caractéristique	Versions de plateforme	Description
Logging (journalisation)	7.0(1)	Fournit des informations de journalisation sur le réseau ASA par le biais de diverses destinations de sortie, et comprend l'option permettant d'afficher et d'enregistrer les fichiers journaux.
Limite de débit	7.0(4)	Limite le débit auquel les messages de journal système sont générés. Nous avons introduit la commande suivante : **logging rate-limit**.

Nom de la caractéristique	Versions de plateforme	Description
Liste de journalisation	7.2(1)	Crée une liste de journalisation à utiliser dans d'autres commandes pour spécifier les messages selon divers critères (niveau de journalisation, classe d'événement et ID de message). Nous avons introduit la commande suivante : **logging list**.
Journalisation de sécurité	8.0(2)	Indique que la connexion à l'hôte de journalisation distant doit utiliser SSL/TLS. Cette option est valide uniquement si le protocole sélectionné est TCP. Nous avons modifié la commande suivante : **logging host**.
Classe de journalisation	8.0(4), 8.1(1)	Ajout de la prise en charge de la classe d'événements ipaa des messages de journalisation. Nous avons modifié la commande suivante : **logging class**.
Classe de journalisation et tampons de journalisation enregistrés	8.2(1)	Ajout de la prise en charge de la classe d'événements dap des messages de journalisation. Nous avons modifié la commande suivante : **logging class**. Ajout de prise en charge pour effacer les tampons de journalisation enregistrés (ASDM, internes, FTP et flash). Nous avons introduit la commande suivante : **clear logging queue bufferwrap**.
Chiffrement de mot de passe	8.3(1)	Ajout de la prise en charge du chiffrement de mot de passe. Nous avons modifié la commande suivante : **logging ftp server**.
Visionneuses de journaux	8.3(1)	Les adresses IP sources et de destination ont été ajoutées aux visionneuses de journaux.
Journalisation et blocage des connexions améliorés	8.3(2)	Lorsque vous configurez un serveur de journal système pour utiliser TCP et que ce serveur n'est pas disponible, l'ASA bloque les nouvelles connexions qui génèrent des messages de journal système jusqu'à ce que le serveur soit à nouveau disponible (par exemple, les connexions VPN, pare-feu et mandataire direct). Cette fonctionnalité a été améliorée pour bloquer également les nouvelles connexions lorsque la file d'attente de journalisation sur l'ASA est pleine; les connexions reprendront lorsque la file d'attente de journalisation sera effacée. Cette fonctionnalité a été ajoutée pour la conformité aux Common Criteria EAL4+. Sauf si nécessaire, nous avons conseillé d'autoriser les connexions lorsque les messages de journal système ne peuvent pas être envoyés ou reçus. Pour autoriser les connexions, continuez à utiliser la commande **logging permit-hostdown**. Nous avons introduit les messages de journal système suivants : 414005, 414006, 414007 et 414008. Nous avons modifié la commande suivante : **show logging**.

Nom de la caractéristique	Versions de plateforme	Description
Filtrage et tri des messages de journal système	v 8.4(1)	Une prise en charge a été ajoutée pour les éléments suivants : • Filtrage des messages de journal système en fonction de plusieurs chaînes de texte correspondant à différentes colonnes • Création de filtres personnalisés • Tri des messages par colonne. Pour en savoir plus, consultez le guide de configuration ASDM. Cette fonctionnalité est compatible avec toutes les versions d'ASA.
Mise en grappe	9.0(1)	Ajout de la prise en charge de la génération de messages de journal système dans un environnement de grappe sur l'ASA 5580 et 5585-X. Nous avons modifié la commande suivante : **logging device-id**.
Blocage des journaux système sur une unité de secours	9.4(1)	Nous avons ajouté la prise en charge du blocage de la génération de messages de journal système spécifiques sur l'unité de secours dans une configuration de basculement. Nous avons introduit la commande suivante : **logging message** *syslog-id* **standby**.
Identités de référence pour les connexions au serveur de journal système sécurisé	9.6(2)	Le traitement du client TLS prend désormais en charge les règles de vérification de l'identité de serveur définies dans la RFC 6125, section 6. La vérification de l'identité sera effectuée pendant la validation PKI pour les connexions TLS au serveur de journal système. Si l'identité présentée ne correspond pas à l'identité de référence configurée, la connexion n'est pas établie. Nous avons ajouté ou modifié les commandes suivantes : **[no] crypto ca reference-identity**, **logging host**.
Prise en charge des adresses IPv6 pour les serveurs de journal système	9.7(1)	Vous pouvez maintenant configurer des serveurs de journal système avec des adresses IPv6 pour enregistrer, envoyer et recevoir des journaux système sur TCP et UDP. Nous avons modifié la commande suivante : **logging host**
Classe de journalisation	9.12(1)	Ajout de la prise en charge de la BFD, du BGP, de l'interface, de l'IPv6, de la multidiffusion, de la commande Object-Group-Search, du PBR, du routage et de la classe SLA des messages de journalisation. Nous avons modifié la commande suivante : **logging class**.
Prise en charge de l'interface de boucle avec retour pour le journal système	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour le journal système. Commandes nouvelles/modifiées : **interface loopback**, **logging host**



CHAPITRE 48

MIB SNMP

Ce chapitre décrit comment configurer le protocole simple de gestion de réseau (SNMP) pour superviser l'ASA.

- À propos de SNMP, à la page 1455
- Lignes directrices pour SNMP, à la page 1471
- Configurer SNMP, à la page 1476
- Supervision SNMP, à la page 1486
- Exemples de SNMP, à la page 1487
- Historique de SNMP, à la page 1488

À propos de SNMP

SNMP est un protocole de couche d'application qui facilite l'échange d'informations de gestion entre les appareils réseau et fait partie de la suite de protocoles TCP /IP. L'ASA prend en charge la surveillance du réseau à l'aide des versions SNMP 1, 2c et 3 de SNMP, et prend en charge l'utilisation des trois versions simultanément. L'agent SNMP qui s'exécute sur l'interface ASA vous permet de surveiller les périphériques réseau à l'aide de systèmes de gestion par réseau (Network Management Systems ou NMS), comme HP OpenView. L'ASA prend en charge l'accès SNMP en lecture seule par l'émission d'une requête GET. L'accès en écriture SNMP n'est pas autorisé, vous ne pouvez donc pas effectuer de modifications avec SNMP. En outre, la requête SNMP SET n'est pas prise en charge.

Vous pouvez configurer la ASA pour envoyer des déroutements, qui sont des messages non sollicités du périphérique géré vers le poste de gestion pour certains événements (notifications d'événement) à un système de gestion de réseau, ou vous pouvez utiliser le système de gestion de réseau pour parcourir les bases d'information de gestion (MIB) sur le périphériques de sécurité. Les MIB sont un ensemble de définitions, et les ASA gèrent une base de données de valeurs pour chaque définition. Parcourir une MIB signifie émettre une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir du système NMS pour déterminer les valeurs.

Remarque Avec des charges de travail intensives, le déploiement de plus de 10 NMS peut avoir une incidence sur les performances de l'appareil. Pour assurer la stabilité et la réactivité de l'appareil, nous vous conseillons d'utiliser avec prudence NMS pour effectuer des interrogations SNMP et gérer le trafic d'interruption.

Les ASA possèdent un agent SNMP qui informe les stations de gestion désignées si des événements prédéfinis nécessitent une notification, par exemple, lorsqu'une liaison du réseau monte ou tombe en panne. La notification

qu'il envoie comprend un OID SNMP, qui s'identifie aux stations de gestion. L'agent ASA répond également lorsqu'une station de gestion demande des renseignements.

Terminologie SNMP

Le tableau suivant répertorie les termes couramment utilisés avec SNMP.

Tableau 63 : Terminologie SNMP

Terme	Description
Agent	Le serveur SNMP exécuté sur ASA. L'agent SNMP présente les caractéristiques suivantes : • Répond aux demandes d'informations et d'actions de le poste de gestion de réseau. • Contrôle l'accès à sa base d'information de gestion, l'ensemble d'objets que le gestionnaire SNMP peut afficher ou modifier. • N'autorise pas les opérations SET.
Navigation	Surveille l'intégrité d'un périphérique à partir de le poste de gestion de réseau en interrogeant les informations requises de l'agent SNMP sur le périphérique. Cette activité peut comprendre l'émission d'une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir de le poste de gestion de réseau afin de déterminer les valeurs.
Bases d'informations de gestion (MIB)	Structures de données normalisées pour la collecte d'informations sur les paquets, les connexions, les tampons, les basculements, etc. Les MIB sont définies par le produit, les protocoles et les normes matérielles utilisés par la plupart des périphériques réseau. Les stations de gestion de réseau SNMP peuvent parcourir les MIB et demander l'envoi de données ou d'événements précis au fur et à mesure qu'ils se produisent.
Postes de gestion de réseau (NSM, Network Management Station)	Les ordinateurs ou postes de travail configurés pour superviser les événements SNMP et gérer les périphériques, tels que l'ASA
Identifiant d'objet (OID)	Le système qui identifie un appareil auprès de son système de gestion système et indique aux utilisateurs la source des renseignements surveillés et affichés.
Trap	Événements prédéfinis qui génèrent un message de l'agent SNMP au système NMS. Les événements comprennent des conditions d'alarme telles qu'un démarrage, un retrait, un démarrage à froid, un démarrage à chaud, une authentification ou des messages syslog.

MIB et déroutements

Les MIB sont standard ou spécifiques à l'entreprise. Les MIB standard sont créées par l'IETF et documentées dans diverses RFC. Un déroutement signale des événements importants se produisant sur un périphérique réseau, le plus souvent des erreurs ou des défaillances. Les déroutements SNMP sont définies dans les MIB standard ou spécifiques à l'entreprise. Les déroutements standard sont créés par l'IETF et documentés dans diverses normes RFC. Les déroutements de SNMP sont compilés dans le logiciel ASA.

Si nécessaire, vous pouvez également télécharger des RFC, des MIB standard et des déroutements standard à partir des emplacements suivants :

http://www.ietf.org/

Parcourez la liste complète des MIB, des déroutements et des OID de Cisco à partir de l'emplacement suivant :

https://github.com/cisco/cisco-mibs/blob/main/supportlists/asa/asa-supportlist.html

Téléchargez également les OID de Cisco par FTP à partir de l'emplacement suivant :

https://github.com/cisco/cisco-mibs/tree/main/oid

Remarque Dans les versions logicielles 7.2(1), 8.0(2) et ultérieures, les renseignements sur l'interface accessibles par SNMP sont actualisés toutes les 5 secondes. Par conséquent, nous vous conseillons d'attendre au moins 5 secondes entre des interrogations consécutives.

Tous les OID des MIB ne sont pas pris en charge. Pour obtenir une liste des MIB et OID SNMP pris en charge pour un ASA en particulier, utilisez la commande suivante :

```
ciscoasa(config)# show snmp-server oidlist
```

Remarque Bien que le mot clé **oidlist** n'apparaisse pas dans la liste d'options de l'aide sur la commande **show snmp-server**, il est disponible. Cependant, cette commande est destinée à l'utilisation de Cisco TAC uniquement. Communiquez avec le centre d'assistance technique (TAC) de Cisco avant d'utiliser cette commande.

Voici un exemple de sortie de la commande **show snmp-server oidlist** :

```
ciscoasa(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.        sysDescr
[1]     1.3.6.1.2.1.1.2.        sysObjectID
[2]     1.3.6.1.2.1.1.3.        sysUpTime
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
```

```
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

Identifiants d'objet SNMP

Chaque produit Cisco de niveau système a un identifiant d'objet SNMP (OID) à utiliser comme sysObjectID MIB-II. Les commandes CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB comprennent les OID qui peuvent être signalés dans l'objet sysObjectID de SNMPv2-MIB, Entity Sensor MIB et Entity Sensor Threshold Ext MIB. Vous pouvez utiliser cette valeur pour identifier le type de modèle. Le tableau suivant répertorie les OID sysObjectID pour les modèles ASA et ISA.

Tableau 64 : Identifiants d'objet SNMP

Identifiant de produit	sysObjectID	Numéro de modèle
ASA virtuel	ciscoASAv (ciscoProducts 1902)	Appareil virtuel de sécurité adaptable Cisco (ASA virtuel)
Contexte système ASA virtuel	ciscoASAvsy (ciscoProducts 1903)	Contexte système de l'appareil virtuel de sécurité adaptable Cisco (ASA virtuel)
Contexte de sécurité ASA virtuel	ciscoASAvsc (ciscoProducts 1904)	Contexte de sécurité de l'appareil virtuel de sécurité adaptable Cisco (ASA virtuel)
Appareil de sécurité industrielle ISA30004C	ciscoProducts 2268	ciscoISA30004C
CISCO ISA30004C avec 4 contextes de sécurité GE en cuivre	ciscoProducts 2139	ciscoISA30004Csc
CISCO ISA30004C avec 4 contextes système GE en cuivre	ciscoProducts 2140	ciscoISA30004Csy
Appareil de sécurité industrielle ISA30002C2F	ciscoProducts 2267	ciscoISA30002C2F
CISCO ISA30002C2F avec 2 ports GE en cuivre + 2 contextes de sécurité GE en fibre	ciscoProducts 2142	ciscoISA30002C2Fsc
CISCO ISA30002C2F avec 2 ports GE en cuivre + 2 contextes système GE en fibre	ciscoProducts 2143	ciscoISA30002C2Fsy
Châssis de l'appareil de sécurité industrielle (ISA) Cisco 30004C	cevChassis 1677	cevChassisISA30004C
Châssis de l'appareil de sécurité industrielle (ISA) Cisco 30002C2F	cevChassis 1678	cevChassisISA30002C2F
Capteur de température de l'unité de traitement Central pour l'UGS ISA30004C en cuivre	cevSensor 187	cevSensorISA30004CCpuTempSensor
Capteur de température de l'unité de traitement Central pour ISA30002C2F en fibre	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
Capteur de température de carte de processeur pour l'UGS ISA30004C en cuivre	cevSensor 192	cevSensorISA30004CPTS
Capteur de température de carte de processeur pour l'UGS ISA30002C2F en fibre	cevSensor 193	cevSensorISA30002C2FPTS

Identifiant de produit	sysObjectID	Numéro de modèle
Capteur de température de carte d'alimentation pour l'UGS ISA30004C en cuivre	cevSensor 197	cevSensorISA30004CPowercardTS
Capteur de température de carte d'alimentation pour l'UGS ISA30002C2F en fibre	cevSensor 198	cevSensorISA30002C2FPowercardTS
Capteur de température de carte de port pour ISA30004C	cevSensor 199	cevSensorISA30004CPortcardTS
Capteur de température de carte de port pour ISA30002C2F	cevSensor 200	cevSensorISA30002C2FPortcardTS
Unité de traitement Central pour l'UGS ISA30004C en cuivre	cevModuleCpuType 329	cevCpuISA30004C
Unité de traitement Central pour l'UGS ISA30002C2F en fibre	cevModuleCpuType 330	cevCpuISA30002C2F
Modules ISA30004C, ISA30002C2F	cevModule 111	cevModuleISA3000Type
Disque SSD pour appareil de sécurité industrielle 30004C	cevModuleISA3000Type 1	cevModuleISA30004CSSD64
Disque SSD pour appareil de sécurité industrielle 30002C2F	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64
Contournement matériel Cisco ISA30004C/ISA30002C2F	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass
Appareil de sécurité FirePOWER 4140, 1U avec module de sécurité intégré 36	ciscoFpr4140K9 (ciscoProducts 2293)	FirePOWER 4140
Appareil de sécurité FirePOWER 4120, 1U avec module de sécurité intégré 24	ciscoFpr4120K9 (ciscoProducts 2294)	FirePOWER 4120
Baie de ventilateur FirePOWER 4K	cevContainer 363	cevContainerFPR4KFanBay
Baie d'alimentation FirePOWER 4K	cevContainer 364	cevContainerFPR4KPowerSupplyBay
Cisco Cisco Secure Firewall Threat Defense Virtual , VMWare	cevChassis 1795	cevChassisCiscoFTDVVMW
Cisco Firewall Threat Defense Virtual, AWS	cevChassis 1796	cevChassisCiscoFTDVAWS

Valeurs de type de prestataire physique

Chaque châssis ou système autonome Cisco a un numéro de type unique pour l'utilisation de SNMP. Les OID entPhysicalVendorType sont définis dans CISCO-ENTITY-VENDORTYPE-OID-MIB. Cette valeur est

renvoyée dans l'objet entPhysicalVendorType à partir de l'agent SNMP ASA, ASA virtuel ou ASASM. Vous pouvez utiliser cette valeur pour identifier le type de composant (module, alimentation, ventilateur, capteurs, CPU, etc.). Le tableau suivant répertorie les valeurs de type de prestataire physique pour les modèles ASA.

Tableau 65 : Valeurs de type de prestataire physique

Article	Description de l'OID entPhysicalVendorType
Port Gigabit Ethernet	cevPortGe (cevPort 109)
Appareil virtuel de sécurité adaptable Cisco	cevChassisASAv (cevChassis 1451)

Tableaux et objets pris en charge dans les MIB

Le tableau suivant répertorie les tableaux et les objets pris en charge pour les MIB précisées.

En mode de contexte multiple, ces tableaux et objets fournissent des renseignements sur un contexte unique. Si vous souhaitez des données dans tous les contextes, vous devez les résumer. Par exemple, pour obtenir l'utilisation générale de la mémoire, effectuez la somme des valeurs cempMemPoolHCUsed pour chaque contexte.

Tableau 66 : Tableaux et objets pris en charge dans les MIB

Nom et OID de MIB	Tableaux et objets pris en charge
CISCO-ENHANCED-MEMPOOL-MIB; OID : 1.3.6.1.4.1.9.9.221	cempMemPoolTable, cempMemPoolIndex, cempMemPoolType, cempMemPoolName, cempMemPoolAlternate, cempMemPoolValid. Pour un système de mémoire de 32 bits, interrogez à l'aide des compteurs de mémoire de 32 bits : cempMemPoolUsed, cempMemPoolFree,cempMemPoolUsedOvrflw, cempMemPoolFreeOvrflw, cempMemPoolLargestFree, cempMemPoolLowestFree, cempMemPoolUsedLowWaterMark, cempMemPoolAllocHit, cempMemPoolAllocMiss, cempMemPoolFreeHit, cempMemPoolFreeMiss, cempMemPoolLargestFreeOvrflw, cempMemPoolLowestFreeOvrflw, cempMemPoolUsedLowWaterMarkOvrflw, cempMemPoolSharedOvrflw. Pour un système de mémoire de 64 bits, interrogez à l'aide des compteurs de mémoire de 64 bits : cempMemPoolHCUsed, cempMemPoolHCFree, cempMemPoolHCLargestFree, cempMemPoolHCLowestFree, cempMemPoolHCUsedLowWaterMark, cempMemPoolHCShared
CISCO-REMOTE-ACCESS-MONITOR-MIB; OID : 1.3.6.1.4.1.9.9.392 **Remarque** Ces trois OID de MIB peuvent être utilisés pour déterminer les raisons pour lesquelles les connexions d'accès à distance échouent.	crasNumTotalFailures, crasNumSetupFailInsufResources, crasNumAbortedSessions
CISCO-ENTITY-SENSOR-EXT-MIB; OID : 1.3.6.1.4.1.9.9.745	ceSensorExtThresholdTable

Nom et OID de MIB	Tableaux et objets pris en charge
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB; OID : 1.3.6.1.4.1.9.9.480	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB; OID : 1.3.6.1.4.1.9.9.720 **Remarque** Non pris en charge sur l'ASA virtuel	ctsxSxpGlobalObjects, ctsxSxpConnectionObjects, ctsxSxpSgtObjects
DISMAN-EVENT-MIB; OID : 1.3.6.1.2.1.88	mteTriggerTable, mteTriggerThresholdTable, mteObjectsTable, mteEventTable, mteEventNotificationTable
DISMAN-EXPRESSION-MIB; OID : 1.3.6.1.2.1.90	expExpressionTable, expObjectTable, expValueTable
ENTITY-SENSOR-MIB; OID : 1.3.6.1.2.1.99 **Remarque** Fournit des renseignements sur les capteurs physiques, comme la température du châssis, le régime des ventilateurs, la tension d'alimentation, etc. Non pris en charge sur la plateforme ASA virtuel.	entPhySensorTable
NAT-MIB; OID : 1.3.6.1.2.1.123	natAddrMapTable, natAddrMapIndex, natAddrMapName, natAddrMapGlobalAddrType, natAddrMapGlobalAddrFrom, natAddrMapGlobalAddrTo, natAddrMapGlobalPortFrom, natAddrMapGlobalPortTo, natAddrMapProtocol, natAddrMapAddrUsed, natAddrMapRowStatus
CISCO-PTP-MIB; OID : 1.3.6.1.4.1.9.9.760 **Remarque** Seules les MIB correspondant au mode d'horloge E2E transparent sont prises en charge.	ciscoPtpMIBSystemInfo, cPtpClockDefaultDSTable, cPtpClockTransDefaultDSTable, cPtpClockPortTransDSTable
CISCO-PROCESS-MIB; 1.3.6.1.4.1.9.9.109.1.1.1.1.7.1 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 to 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	cpmCPUTotal1minRev Paramètres associés et valeurs de cPMCPUTotal1minRev Exemples : • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) : pourcentage d'utilisation de la CPU agrégé du système (cette valeur est identique à l'utilisation de la CPU du système de la version .3.6.1.4.1.9.9.109.1.1.1.1.7.1 en mode contexte unique). • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) : pourcentage d'utilisation moyenne du processeur Snort (valeur agrégée totale de toutes les instances Snort) • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) : pourcentage moyen de processus système (moyenne des cœurs « Sysprocess »)

Interruptions prises en charge (notifications)

Le tableau suivant répertorie les interruptions prises en charge (notifications) et les MIB associées.

Tableau 67 : Interruptions prises en charge (notifications)

Nom de l'interruption et de la MIB	Liste des variables	Description
authenticationFailure (SNMPv2-MIB)	—	Pour SNMP version 1 ou 2, l'identifiant de communauté fourni dans la demande SNMP est incorrect. Pour SNMP version 3, une PDU de rapport est générée au lieu d'une interruption si les mots de passe ou les noms d'utilisateur de l'authentification ou du privilège sont incorrects. La commande **snmp-server enable traps snmp authentication** est utilisée pour activer et désactiver la transmission de ces interruptions.
bgpBackwardTransition	bgpPeerLastError, bgpPeerState	La commande **snmp-server enable traps peer-flap** est utilisée pour activer la transmission des interruptions BGP homologues.
ccmCLIRunningConfigChanged (CISCO-CONFIG-MAN-MIB)	ccmHistoryRunningLastChanged, ccmHistoryEventTerminalType	La commande **snmp-server enable traps config** est utilisée pour activer la transmission de cette interruption.
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	La commande **snmp-server enable traps entity fru-insert** est utilisée pour activer cette notification.
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	La commande **snmp-server enable traps entity fru-remove** est utilisée pour activer cette notification.

Nom de l'interruption et de la MIB	Liste des variables	Description
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)	entPhysicalName, entPhysicalDescr, entPhySensorValue, entPhySensorType, ceSensorExtThresholdValue	La commande **snmp-server enable traps entity** [**power-supply-failure** | **fan-failure** | **cpu-temperature**] est utilisée pour activer la transmission des notifications de seuil d'entité. Cette notification est envoyée en cas de défaillance de l'alimentation. Les objets envoyés identifient la température du ventilateur et du processeur. La commande **snmp-server enable traps entity fan-failure** est utilisée pour activer la transmission de l'interruption de défaillance du ventilateur.Cette interruption ne s'applique pas à la série Firepower 2100. La commande **snmp-server enable traps entity power-supply-failure** est utilisée pour activer la transmission de l'interruption de défaillance de l'alimentation.Cette interruption ne s'applique pas à la série Firepower 2100. La commande **snmp-server enable Traps entités châssis-ventilateur** est utilisée pour activer la transmission de l'interruption de défaillance du ventilateur du châssis. La commande **snmp-server enable traps entity cpu-temperature** est utilisée pour activer la transmission de l'interruption de température CPU élevée. Cette interruption ne s'applique pas à la série Firepower 2100. La commande **snmp-server enable traps entity power-supply-presence** est utilisée pour activer la transmission de l'interruption de défaillance de la présence de l'alimentation. La commande **snmp-server enable traps entity power-supply-temperature** est utilisée pour activer la transmission de l'interruption de seuil de température de l'alimentation. La commande **snmp-server enable traps entity chassis-temperature** est utilisée pour activer la transmission de l'interruption de la température ambiante du châssis. Cette interruption ne s'applique pas à la série Firepower 2100. La commande **snmp-server enable traps entity accelerator-temperature** est utilisée pour activer la transmission de l'interruption de la température de l'accélérateur du châssis.

Nom de l'interruption et de la MIB	Liste des variables	Description
cikeTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr, cikePeerRemoteAddr, cikeTunLifeTime	La commande **snmp-server enable traps ikev2 start** est utilisée pour activer la transmission de l'interruption de démarrage ikev2.
cikeTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr, cikePeerRemoteAddr, cikeTunActiveTime	La commande **snmp-server enable traps ikev2 stop** est utilisée pour activer la transmission de l'interruption d'arrêt ikev2.
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime, cipSecTunLifeSize	La commande **snmp-server enable traps ipsec start** est utilisée pour activer la transmission de cette interruption.
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	La commande **snmp-server enable traps ipsec stop** est utilisée pour activer la transmission de cette interruption.
ciscoConfigManEvent (CISCO-CONFIG-MAN-MIB)	ccmHistoryEventCommandSource, ccmHistoryEventConfigSource, ccmHistoryEventConfigDestination	La commande **snmp-server enable traps config** est utilisée pour activer la transmission de cette interruption.
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions, crasNumUsers, crasMaxSessionsSupportable, crasMaxUsersSupportable, crasThrMaxSessions	La commande **snmp-server enable traps remote-access session-threshold-exceeded** est utilisée pour activer la transmission de ces interruptions.
ciscoUFwFailoverStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	gid, FOStatus	La commande **snmp-server enable traps failover-state** est utilisée pour activer la transmission de l'interruption d'état du basculement.
clogMessageGenerated (CISCO-SYSLOG-MIB)	clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp	Des messages de journal système sont générés. La valeur de l'objet clogMaxSeverity est utilisée pour décider quels messages de journal système sont envoyés en tant qu'interruptions. La commande **snmp-server enable traps syslog** est utilisée pour activer et désactiver la transmission de ces interruptions.
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType, crlResourceLimitMax, clogOriginIDType, clogOriginID	La commande **snmp-server enable traps connection-limit-reached** est utilisée pour activer la transmission de la notification de limite de connexion atteinte. L'objet clogOriginID comprend le nom du contexte à partir duquel provient l'interruption.

Nom de l'interruption et de la MIB	Liste des variables	Description
coldStart (SNMPv2-MIB)	—	L'interruption coldStart qui se produit lorsque l'agent SNMP démarre après la configuration de SNMP. Cette interruption se produit également lorsque l'agent démarre après un redémarrage du système. **Remarque** Pour les nœuds de grappe et de haute disponibilité, publiez un rechargement, si le temps de redémarrage des interfaces dépasse 5 minutes (seuil de présélection), l'interruption est abandonnée. Lorsque la grappe et les nœuds à haute disponibilité ont redémarré avec succès, toutes les autres interruptions sont envoyées comme prévu. La commande **snmp-server enable traps snmp coldstart** est utilisée pour activer et désactiver la transmission de ces interruptions.
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue, cpmCPUTotalMonIntervalValue, cpmCPUInterruptMonIntervalValue, cpmCPURisingThresholdPeriod, cpmProcessTimeCreated, cpmProcExtUtil5SecRev	La commande **snmp-server enable traps cpu threshold rising** est utilisée pour activer la transmission de la notification d'augmentation du seuil de CPU. L'objet cpmCPURisingThresholdPeriod est envoyé avec les autres objets.
cufwClusterStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	status	La commande **snmp-server enable traps cluster-state** est utilisée pour activer la transmission de l'interruption d'état de la grappe.
entConfigChange (ENTITY-MIB)	—	La commande **snmp-server enable traps entity config-change fru-insert fru-remove** est utilisée pour activer cette notification. **Remarque** Cette notification est envoyée uniquement en multimode, lorsqu'un contexte de sécurité est créé ou supprimé.
linkDown (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	L'interruption linkdown (perte de liaison) pour les interfaces. La commande **snmp-server enable traps snmp linkdown** est utilisée pour activer et désactiver la transmission de ces interruptions.
linkUp (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	L'interruption linkup (établissement de liaison) pour les interfaces. La commande **snmp-server enable traps snmp linkup** est utilisée pour activer et désactiver la transmission de ces interruptions.

Nom de l'interruption et de la MIB	Liste des variables	Description
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, cempMemPoolName, cempMemPoolHCUsed	La commande **snmp-server enable traps memory-threshold** est utilisée pour activer la notification de seuil de mémoire. Le mteHotOID est défini sur cempMemPoolHCUsed. Les objets cempMemPoolName et cempMemPoolHCUsed sont envoyés avec les autres objets.
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, ifHCInOctets, ifHCOutOctets, ifHighSpeed, entPhysicalName	La commande **snmp-server enable traps interface-threshold** est utilisée pour activer la notification de seuil d'interface. Les objets entPhysicalName sont envoyés avec les autres objets.
natPacketDiscard (NAT-MIB)	ifIndex	La commande **snmp-server enable traps nat packet-discard** est utilisée pour activer la notification de suppression de paquet NAT. Cette notification est limitée pendant 5 minutes et est générée lorsque les paquets IP sont rejetés par la NAT en raison de l'espace de mappage non disponible. L'ifIndex donne l'ID de l'interface mappée.
ospfNbrStateChange	ospfRouterId, ospfNbrIpAddr, ospfNbrAddressLessIndex, ospfNbrRtrId, ospfNbrState	La commande **snmp-server enable traps peer-flap** est utilisée pour activer la transmission des pièges OSPF homologues. **Remarque** Pour les modèles ASA5585, le moteur SNMP est modifié pour utiliser la bibliothèque netsnmp version 5.8 et les OID suivants ne sont pas disponibles dans la bibliothèque : • ospfIfStateChange 1.3.6.1.2.1.14.16.2.16 • ospfVirtIfStateChange 1.3.6.1.2.1.14.16.2.1 • ospfVirtNbrStateChange 1.3.6.1.2.1.14.16.2.3
warmStart (SNMPv2-MIB)	—	L'interruption warmStart qui se produit lorsque l'agent SNMP redémarre pour la première fois. Cette interruption se produit également lorsque l'agent redémarre après une modification de configuration SNMP, où toutes les configuration d'hôte SNMP sont supprimées et une nouvelle configuration SNMP est effectuée. La commande **snmp-server enable traps snmp warmstart** est utilisée pour activer et désactiver la transmission de ces interruptions.

Types d'interface et exemples

Voici les types d'interfaces qui produisent les statistiques de trafic SNMP :

- Logique : statistiques recueillies par le pilote logiciel, qui constituent un sous-ensemble de statistiques physiques.
- Physique : statistiques recueillies par le pilote matériel. Chaque interface physique nommée est associée à un ensemble de statistiques logiques et physiques. Chaque interface physique peut être associée à plusieurs interfaces VLAN. Les interfaces VLAN n'ont que des statistiques logiques.



Remarque Pour une interface physique qui est associée à plusieurs interfaces VLAN, sachez que les compteurs SNMP pour les OID ifInOctets et ifOutoctets correspondent aux compteurs de trafic agrégé pour cette interface physique.

- VLAN uniquement : SNMP utilise les statistiques logiques pour ifInOctets et ifOutOctets.

Les exemples du tableau suivant montrent les différences entre les statistiques de trafic SNMP. L'exemple 1 montre la différence entre les statistiques de sortie physiques et logiques des commandes **show interface** et **show traffic**. L'exemple 2 présente les statistiques de sortie d'une interface VLAN uniquement pour les commandes **show interface** et **show traffic**. L'exemple montre que les statistiques sont proches de la sortie qui s'affiche pour la commande **show traffic**.

Tableau 68 : Statistiques de trafic SNMP pour les interfaces physiques et VLAN

Exemple 1	Exemple 2
ciscoasa# **show interface GigabitEthernet3/2** interface GigabitEthernet3/2 description fullt-mgmt nameif mgmt security-level 10 ip address 10.7.14.201 255.255.255.0 management-only ciscoasa# **show traffic** (Condensed output) Physical Statistics GigabitEthernet3/2: received (in 121.760 secs) **36 packets 3428 bytes** 0 pkts/sec 28 bytes/sec Logical Statistics mgmt: received (in 117.780 secs) **36 packets 2780 bytes** 0 pkts/sec 23 bytes/sec Les exemples suivants montrent les statistiques de sortie SNMP pour l'interface de gestion et l'interface physique. La valeur ifInOctets est proche de la sortie des statistiques physiques qui apparaît dans la sortie de la commande **show traffic**, mais pas de la sortie des statistiques logiques. ifIndex de l'interface de gestion : IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt' interface ifInOctets correspondant aux statistiques de l'interface physique : **IF-MIB::ifInOctets.6 = Counter32:3246**	ciscoasa# **show interface GigabitEthernet0/0.100** interface GigabitEthernet0/0.100 vlan 100 nameif inside security-level 100 ip address 10.7.1.101 255.255.255.0 standby 10.7.1.102 ciscoasa# **show traffic** inside received (in 9921.450 secs) **1977 packets 126528 bytes** 0 pkts/sec 12 bytes/sec transmitted (in 9921.450 secs) **1978 packets 126556 bytes** 0 pkts/sec 12 bytes/sec ifIndex du VLAN interne : IF-MIB::ifDescr.9 = Adaptive Security Appliance 'inside' interface **IF-MIB::ifInOctets.9 = Counter32: 126318**

Présentation du SNMP version 3

SNMP version 3 offre des améliorations de sécurité qui ne sont pas disponibles dans les versions SNMP 1 et 2c. Les versions SNMP 1 et 2c transmettent des données entre le serveur SNMP et l'agent SNMP en texte clair. SNMP version 3 ajoute des options d'authentification et de confidentialité pour sécuriser les opérations du protocole. En outre, cette version contrôle l'accès à l'agent SNMP et aux objets MIB par le biais du modèle de sécurité basé sur l'utilisateur (USM) et du modèle de contrôle d'accès basé sur l'affichage (VACM). L'ASA prend également en charge la création de groupes SNMP et d'utilisateurs, ainsi que d'hôtes, ce qui est nécessaire pour activer l'authentification et le chiffrement du transport pour des communications SNMP sécurisées.

Modèles de sécurité

À des fins de configuration, les options d'authentification et de confidentialité sont regroupées dans des modèles de sécurité. Les modèles de sécurité s'appliquent aux utilisateurs et aux groupes, qui sont répartis dans les trois types suivants :

- NoAuthPriv : pas d'authentification ni de confidentialité, ce qui signifie qu'aucune sécurité n'est appliquée aux messages.
- AuthNoPriv : authentification mais pas de confidentialité, ce qui signifie que les messages sont authentifiés.
- AuthPriv : authentification et confidentialité, ce qui signifie que les messages sont authentifiés et chiffrés.

SNMP Groups (groupes SNMP)

Un groupe SNMP est une stratégie de contrôle d'accès à laquelle des utilisateurs peuvent être ajoutés. Chaque groupe SNMP est configuré avec un modèle de sécurité et est associé à une vue SNMP. Un utilisateur appartenant à un groupe SNMP doit correspondre au modèle de sécurité du groupe SNMP. Ces paramètres spécifient le type d'authentification et de confidentialité utilisé par un utilisateur appartenant à un groupe SNMP. Chaque paire de noms de groupes SNMP et de modèles de sécurité doit être unique.

Utilisateurs SNMP

Les utilisateurs SNMP disposent d'un nom d'utilisateur spécifié, d'un groupe auquel ils appartiennent, d'un mot de passe d'authentification, d'un mot de passe de chiffrement et d'algorithmes d'authentification et de chiffrement à utiliser. Les options d'algorithme d'authentification sont SHA-1, SHA-224, SHA-256 HMAC et SHA-384. Les options d'algorithme de chiffrement sont 3DES et AES (qui sont disponibles en versions 128, 192 et 256). Lorsque vous créez un utilisateur, vous devez l'associer à un groupe SNMP. L'utilisateur hérite ensuite du modèle de sécurité du groupe.

Remarque Lors de la configuration d'un compte d'utilisateur SNMPv3, assurez-vous que la longueur de l'algorithme d'authentification est égale ou supérieure à la longueur de l'algorithme de chiffrement.

Hôtes SNMP

Un hôte SNMP est une adresse IP à laquelle les notifications et les alertes SNMP sont envoyées. Pour configurer les hôtes SNMP version 3, ainsi que l'adresse IP cible, vous devez configurer un nom d'utilisateur, car les alertes ne sont envoyées qu'à un utilisateur configuré. Les adresses IP cibles SNMP et les noms de paramètre cibles doivent être uniques sur l'ASA. Chaque hôte SNMP ne peut être associé qu'à un seul nom d'utilisateur. Pour recevoir des alertes SNMP, après avoir ajouté la commande **snmp-server host**, assurez-vous de configurer les renseignements d'authentification de l'utilisateur sur le NMS pour qu'ils correspondent aux renseignements d'authentification de l'ASA.

Remarque Vous pouvez ajouter jusqu'à 8 192 hôtes. Cependant, seulement 128 de ceux-cis peuvent être utilisés pour les déroutements.

Différences d'implémentation entre les logiciels ASA et Cisco IOS

La mise en œuvre de SNMP version 3 dans l'ASA diffère de la mise en œuvre de SNMP version 3 dans le logiciel Cisco IOS de la manière suivante :

- Les ID du moteur local et du moteur distant ne sont pas configurables. L'ID du moteur local est généré au démarrage de l'ASA ou lors de la création d'un contexte.
- Aucune prise en charge n'existe pour le contrôle d'accès basé sur l'affichage, ce qui entraîne une navigation MIB non limitée.
- La prise en charge est limitée aux MIB suivantes : USM, VACM, FRAMEWORK et TARGET.
- Vous devez créer des utilisateurs et des groupes avec le modèle de sécurité approprié.
- Vous devez supprimer les utilisateurs, les groupes et les hôtes dans le bon ordre.
- L'utilisation de la commande snmp-server host crée une règle ASA pour autoriser le trafic SNMP entrant.

Messagerie du journal système SNMP

SNMP génère des messages de journal système détaillés, numérotés 212*nnn*. Les messages du journal système indiquent l'état des requêtes SNMP, des interruptions SNMP, des canaux SNMP et des réponses SNMP de l'ASA ou de l'ASASM à un hôte spécifié sur une interface spécifiée.

Pour obtenir des renseignements détaillés sur les messages du journal système, consultez le guide des messages de journal système.

Remarque L'interrogation SNMP échoue si les messages de journal système du protocole SNMP dépassent un débit élevé (environ 4 000 par seconde).

Services d'application et outils tiers

Pour en savoir plus sur la prise en charge de SNMP, consultez l'URL suivante :

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

Pour en savoir plus sur l'utilisation d'outils tiers pour parcourir les MIB de la version 3 du SNMP, consultez l'URL suivante :

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

Lignes directrices pour SNMP

Cette section comprend les lignes directrices et les limites que vous devez consulter avant de configurer SNMP.

Lignes directrices en matière de basculement et de mise en grappe

- Lorsque vous utilisez SNMPv3 avec mise en grappe ou basculement, si vous ajoutez une nouvelle unité de grappe après la formation initiale de la grappe ou si vous remplacez une unité de basculement, les

utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez rajouter les utilisateurs SNMPv3 à l'unité de contrôle ou active pour forcer les utilisateurs à être dupliqués sur la nouvelle unité; ou vous pouvez ajouter les utilisateurs directement sur la nouvelle unité (les utilisateurs et les groupes SNMPv3 sont une exception à la règle selon laquelle vous ne pouvez pas saisir de commandes de configuration sur une unité de données en grappe). Reconfigurez chaque utilisateur en saisissant la commande **snmp-server user** *username group-name* **v3** sur l'unité de contrôle/active ou directement sur l'unité de données/secours avec les options *priv-password* et *auth-password* dans leur format non chiffré.

Lignes directrices relatives à IPv6 (tous les modèles ASA)

SNMP peut être configuré sur le transport IPv6 de sorte qu'un hôte IPv6 puisse exécuter des requêtes SNMP et recevoir des notifications SNMP d'un périphérique exécutant le logiciel IPv6. L'agent SNMP et les MIB associées ont été améliorés pour prendre en charge l'adressage IPv6.

Lignes directrices relatives à IPv6 pour Firepower 2100

Firepower 2100 exécute un système d'exploitation sous-jacent appelé FXOS et prend en charge le mode appareil (par défaut) et le mode plateforme; voir Régler le Firepower 2100 en mode appareil ou plateforme, à la page 37.

En mode plateforme, vous devez configurer une adresse IP de gestion IPv6 dans FXOS. Dans l'exemple suivant, une passerelle et une interface de gestion IPv6 sont configurées :

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
Management IPv6 Interface:
IPv6 Address Prefix IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998 64 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

Directives supplémentaires

- Les interruptions d'alimentation ne sont pas émises pour les systèmes fonctionnant en mode appareil.
- Pour Firepower 2100, en mode plateforme, vous ne pouvez pas interroger les interfaces membres d'un EtherChannel, et les interruptions pour les interfaces membres ne sont pas générées. Cette fonctionnalité est prise en charge si vous activez SNMP directement dans FXOS. Le mode appareil n'est pas affecté.
- Ne prend pas en charge les interruptions ASA pour les membres de ports individuels pour le Firepower 2100 en mode plateforme; consultez le Guide de référence de Cisco Firepower 2100 FXOS MIB.
- Pour Firepower 2100, en mode appareil, vous ne pouvez pas interroger le modèle matériel ni le numéro de série. De plus, dans l'ASA, les interruptions ne sont pas générées pour ces détails. Par conséquent, configurez SNMP sur FXOS ou Chassis Manager pour interroger l'adresse IP de gestion de châssis au lieu des interfaces sur l'instance ASA.
- Vous devez disposer de Cisco Works pour Windows ou d'un autre navigateur conforme à SNMP MIB-II pour recevoir des alertes SNMP ou parcourir une MIB.

- L'accès de gestion sur un tunnel VPN n'est pas pris en charge avec SNMP (la commande **management-access**). Pour SNMP sur VPN, nous vous recommandons d'activer SNMP sur une interface de boucle avec retour. Vous n'avez pas besoin d'activer la fonctionnalité d'accès de gestion pour utiliser SNMP sur l'interface de boucle avec retour. La boucle avec retour fonctionne également pour SSH.
- Ne prend pas en charge le contrôle d'accès basé sur l'affichage, mais il est possible de parcourir la MIB VACM pour déterminer les paramètres d'affichage par défaut.
- ENTITY-MIB n'est pas disponible dans le contexte de non-administration. Utilisez plutôt IF-MIB pour effectuer des requêtes dans le contexte de non-administration.
- ENTITY-MIB n'est pas disponible pour l'Firepower 9300. Utilisez plutôt CISCO-FIREPOWER-EQUIPMENT-MIB et CISCO-FIREPOWER-SM-MIB.
- Sur certains périphériques, il a été observé que l'ordre des interfaces (ifDescr) dans la sortie de **snmpwalk** change après un redémarrage. L'ASA utilise un algorithme pour déterminer le tableau ifIndex que SNMP interroge. Lorsque l'ASA est démarré, les interfaces sont ajoutées au tableau ifIndex dans l'ordre chargé au fur et à mesure que l'ASA lit la configuration. Les nouvelles interfaces ajoutées à l'ASA sont ajoutées à la liste des interfaces dans le tableau ifIndex. Lorsque des interfaces sont ajoutées, supprimées ou renommées, cela peut affecter l'ordre des interfaces lors du redémarrage.
- Lorsque vous fournissez un OID dans la commande **snmpwalk**, l'outil snmpwalk interroge toutes les variables de la sous-arborescence qui se trouve sous l'OID spécifié et affiche leurs valeurs. Ainsi, pour afficher une sortie complète des objets sur le périphérique, assurez-vous de fournir l'OID dans la commande **snmpwalk**.
- Ne prend pas en charge la version 3 du SNMP pour AIP SSM ou AIP SSC.
- Ne prend pas en charge le débogage SNMP.
- Ne prend pas en charge la récupération des renseignements ARP.
- Ne prend pas en charge les commandes SNMP NET.
- Lorsque vous utilisez NET-SNMP version 5.4.2.1, prend uniquement en charge la version de l'algorithme de chiffrement AES128. Ne prend pas en charge les versions des algorithmes de chiffrement AES256 ou AES192.
- Les modifications apportées à la configuration existante sont refusées si le résultat place la fonctionnalité SNMP dans un état incohérent.
- Pour la version 3 de SNMP, la configuration doit avoir lieu dans l'ordre suivant : groupe, utilisateur, hôte.
- Pour Firepower 2100, lorsque SNMPv3 est configuré sur l'interface de gestion des périphériques, tous les utilisateurs de SNMPv3 peuvent interroger le périphérique même lorsqu'ils ne sont pas mappés dans la configuration de l'hôte.
- Pour les modèles Secure Firewall, la commande **snmpwalk** interroge les membres FXOS uniquement à partir du contexte d'administration.
- Avant de supprimer un groupe, vous devez vous assurer que tous les utilisateurs associés à ce groupe sont supprimés.
- Avant de supprimer un utilisateur, vous devez vous assurer qu'aucun hôte associé à ce nom d'utilisateur n'est configuré.

- Si les utilisateurs ont été configurés pour appartenir à un groupe particulier avec un certain modèle de sécurité, et si le niveau de sécurité de ce groupe est modifié, vous devez effectuer les opérations suivantes dans cet ordre :
  - Supprimer les utilisateurs de ce groupe.
  - Modifier le niveau de sécurité du groupe.
  - Ajouter des utilisateurs qui appartiennent au nouveau groupe.
- La création de vues personnalisées pour restreindre l'accès des utilisateurs à un sous-ensemble d'objets MIB n'est pas prise en charge.
- Toutes les requêtes et toutes les interruptions sont disponibles uniquement dans la vue Lecture/Notification par défaut.
- L'interruption de la limite de connexion atteinte est générée dans le contexte d'administration. Pour générer cette interruption, vous devez avoir au moins un hôte de serveur SNMP configuré dans le contexte d'utilisateur dans lequel la limite de connexion a été atteinte.
- Vous pouvez ajouter jusqu'à 4 000 hôtes. Cependant, seulement 128 de ceux-cis peuvent être utilisés pour les déroutements.
- Le nombre total de destinations d'interrogation actives prises en charge est de 128.
- Vous pouvez spécifier un objet réseau pour indiquer les hôtes individuels que vous souhaitez ajouter en tant que groupe d'hôtes.
- Vous pouvez associer plusieurs utilisateurs à un hôte.
- Vous pouvez spécifier des objets réseau qui se chevauchent dans différentes commandes **host-group**. Les valeurs que vous spécifiez pour le dernier groupe d'hôtes s'appliquent à l'ensemble commun d'hôtes dans les différents objets réseau.
- Si vous supprimez un groupe d'hôtes ou des hôtes qui se chevauchent avec d'autres groupes d'hôtes, les hôtes sont reconfigurés en utilisant les valeurs qui ont été spécifiées dans les groupes d'hôtes configurés.
- Les valeurs acquises par les hôtes dépendent de la séquence spécifiée que vous utilisez pour exécuter les commandes.
- La limite de taille des messages que SNMP envoie est de 1 472 octets.
- L'ASA prend en charge un nombre illimité d'hôtes d'interruption de serveur SNMP par contexte. La sortie de la commande **show snmp-server host** affiche uniquement les hôtes actifs qui interrogent l'ASA, ainsi que les hôtes configurés de manière statique.

Astuces de dépannage

- Pour vous assurer que le processus SNMP qui reçoit les paquets entrants du NMS est en cours d'exécution, saisissez la commande suivante :

```
ciscoasa(config)# show process | grep snmp
```

- Pour capturer les messages de journal système provenant du SNMP et les faire apparaître sur la console ASA, saisissez les commandes suivantes :

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(config)# logging console snmp
```

- Pour vous assurer que le processus SNMP envoie et reçoit des paquets, saisissez les commandes suivantes :

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(config)# show snmp-server statistics
```

  La sortie est basée sur le groupe SNMP de SNMPv2-MIB.

- Pour vous assurer que les paquets SNMP passent par l'ASA et parviennent au processus SNMP, saisissez les commandes suivantes :

```
ciscoasa(config)# clear asp drop
ciscoasa(config)# show asp drop
```

- Si le NMS ne parvient pas à demander des objets avec succès ou ne traite pas correctement les interruptions entrantes provenant de l'ASA, utilisez une capture de paquets pour isoler le problème en saisissant les commandes suivantes :

```
ciscoasa (config)# access-list snmp permit udp any eq snmptrap any
ciscoasa (config)# access-list snmp permit udp any any eq snmp
ciscoasa (config)# capture snmp type raw-data access-list snmp interface mgmt
ciscoasa (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

- Si l'ASA ne fonctionne pas comme prévu, obtenez des renseignements sur la topologie du réseau en procédant comme suit :
  - Pour la configuration NMS, obtenez les renseignements suivants :

    Nombre de délais d'expiration

    Nombre de tentatives :

    Mise en mémoire cache de l'ID du moteur

    Nom d'utilisateur et mot de passe utilisés

  - Exécutez les commandes suivantes :

    show block

    show interface

    show process

    show cpu

    show vm

- Si une erreur fatale se produit, pour faciliter la reproduction de l'erreur, envoyez un fichier de recherche de la source et la sortie de la commande **show tech-support** au TAC de Cisco.
- Si le trafic SNMP n'est pas autorisé par les interfaces ASA, vous devrez peut-être également autoriser le trafic ICMP provenant du serveur SNMP distant à l'aide de la commande **icmp permit**.

- Si vous avez configuré le périphérique avec **snmp-server enable oid**, lors des opérations de marche SNMP, l'ASA interrogera les renseignements de mémoire des groupes MEMPOOL_DMA et MEMPOOL_GLOBAL_SHARED. Cela peut entraîner des saturations du CPU liées à SNMP qui peuvent entraîner des abandons de paquet. Pour maîtriser ce problème, évitez d'interroger les OID qui se rapportent au groupe partagé global à l'aide de la commande **no snmp-server enable oid**. Lorsqu'ils sont désactivés, les OID du groupe de mémoire renvoient 0 octet.
- Lorsque vous utilisez SNMPGET avec un grand nombre d'OID dans une seule demande d'interrogation des compteurs d'abandon ASP, une interrogation répétée des compteurs d'abandon ASP se traduit par une utilisation accrue du CPU. Par conséquent, nous vous conseillons de déterminer les compteurs importants à surveiller et à utiliser SNMPGET sur chaque compteur pour obtenir ces valeurs de manière à limiter l'impact sur le CPU.
- Lorsque SNMP est configuré sur plusieurs contextes dans un ASA à contextes multiples, interrogez les contextes de manière séquentielle et utilisez SNMPBULKGET au lieu de snmpwalk pour réduire le nombre de connexions à la plateforme. Cette approche évitera les retards ou les délais d'expiration de SNMP lorsqu'un grand nombre de contextes sont interrogés en même temps.
- L'ASA définit de manière cohérente le bit Don't Fragment (DF) lors de la réponse aux interrogations SNMP avec des messages SNMP get-response, tels que SNMPBULKGET, qui nécessite que l'ensemble du chemin réseau prenne en charge au moins l'unité de transfert maximale (MTU) configurée dans l'ASA. Si une MTU inférieure est configurée sur le chemin réseau, d'autres périphériques peuvent envoyer des paquets ICMP (Internet Control Message Protocol) demandant la fragmentation. Cependant, puisque le bit DF est défini, l'ASA ne répond pas et ne fragmente pas les paquets, ce qui entraîne une perte de réponse de l'ASA.

  Pour résoudre ce problème, vous pouvez modifier la MTU sur l'ASA ou sur l'ensemble du chemin réseau, utiliser plusieurs demandes get au lieu de SNMPBULKGET, ou réduire la taille groupée des demandes SNMPBULKGET.

- Pour en savoir plus sur le dépannage, consultez l'URL suivante : http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

Configurer SNMP

Cette section décrit comment configurer SNMP.

Procédure

Étape 1 Activez l'agent SNMP et le serveur SNMP.

Étape 2 Configurez les alertes SNMP.

Étape 3 Configurez les paramètres SNMP de version 1 et 2c ou les paramètres SNMP de version 3.

Activer l'agent SNMP et le serveur SNMP

Pour activer l'agent SNMP et le serveur SNMP, procédez comme suit :

Procédure

Activez l'agent SNMP et le serveur SNMP sur l'ASA. Par défaut, le serveur SNMP est activé.

snmp-server enable

Exemple :

```
ciscoasa(config)# snmp-server enable
```

Configurer les déroutements SNMP

Pour désigner les interruptions que l'agent SNMP génère et la manière dont elles sont collectées et envoyées aux NMS, procédez comme suit :



Remarque Lorsque vous activez toutes les alertes de SNMP ou de syslog, il est possible que le processus SNMP consomme les ressources excédentaires de l'agent et du réseau, ce qui entraîne le blocage du système. Si vous remarquez des retards du système, des demandes non terminées ou des échéances de délais d'expiration, vous pouvez activer de manière sélective les déroutements SNMP et syslog. Par exemple, vous pouvez ignorer le niveau de gravité *Informational* (Informationnel) de l'interruption de journal système.

Procédure

Envoyez des interruptions individuelles, des ensembles d'interruptions ou toutes les interruptions au NMS.

snmp-server enable traps [**all** | **syslog** | **snmp** [**authentication** | **linkup** | **linkdown** | **coldstart** | **warmstart**] | **config** | **entity** [**config-change** | **fru-insert** | **fru-remove** | **fan-failure** | **cpu-temperature** | **chassis-fan-failure** | **power-supply**] | **chassis-temperature** | **power-supply-presence** | **power-supply-temperature** **l1-bypass-status**] | **ikev2** [**start** | **stop**] | **cluster-state** | **failover-state** | **peer-flap** | **ipsec** [**start** | **stop**] | **remote-access** [**session-threshold-exceeded**] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [**packet-discard**]

Exemple :

```
ciscoasa(config)# snmp-server enable traps snmp authentication
linkup linkdown coldstart warmstart
```

Cette commande permet d'envoyer les messages de journal système en tant qu'interruptions au NMS. Toutes les interruptions standard SNMP sont activées dans la configuration par défaut, comme le montre l'exemple. Pour désactiver ces interruptions, utilisez la commande **no snmp-server enable traps snmp**.

Si vous saisissez cette commande et ne spécifiez pas de type d'interruption, la valeur par défaut est l'interruption **syslog**. Par défaut, l'interruption **syslog** est activée. Les alertes SNMP par défaut continuent d'être activées avec l'interruption **syslog** (journal système).

Vous devez configurer la commande **logging history** (historique de journalisation) et la commande **snmp-server enable traps syslog** pour générer des interruptions à partir de la MIB du journal système.

Pour rétablir l'activation par défaut des alertes SNMP, utilisez la commande **clear configure snmp-server**. Toutes les autres interruptions sont désactivées par défaut.

Interruptions disponibles dans le contexte d'administration uniquement :

- **connection-limit-reached**
- **entity**
- **memory-threshold**

Interruptions générées via le contexte d'administration uniquement pour les interfaces physiquement connectées dans le contexte système :

- **interface-threshold**

Toutes les autres interruptions sont disponibles dans les contextes d'administration et d'utilisateur en mode unique.

L'interruption **config** active les notifications ciscoConfigManEvent et ccmCLIRunningConfigChanged, qui sont générées après avoir quitté le mode de configuration.

Si l'utilisation du CPU est supérieure à la valeur de seuil configurée pour la période de supervision configurée, l'interruption **cpu threshold rising** est générée.

Lorsque la mémoire du contexte système utilisée atteint 80 % de la mémoire totale du système, l'interruption **memory-threshold** est générée à partir du contexte d'administration. Pour tous les autres contextes d'utilisateur, cette interruption est générée lorsque la mémoire utilisée atteint 80 % de la mémoire totale du système dans ce contexte en particulier.

Certains déroutements ne sont pas applicables à certains modèles de matériel. Utilisez ? à la place d'un mot clé d'interruption pour déterminer quelles interruptions sont disponibles pour votre appareil. Par exemple :

- Le Série Firepower 1000 prend uniquement en charge les interruptions d'entité suivantes : **chassis-temperature**, **config-change** et **cpu-temperature**.

Remarque
SNMP ne surveille pas les capteurs de tension.

Configurer un seuil d'utilisation du CPU

Pour configurer un seuil d'utilisation du CPU, procédez comme suit :

Procédure

Configurez la valeur de seuil pour un seuil de CPU élevé et la période de supervision du seuil.

snmp cpu threshold rising *threshold_value monitoring_period*

Exemple :

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

Pour effacer la valeur de seuil et la période de supervision de l'utilisation du CPU, utilisez la forme **no** de cette commande. Si la commande **snmp cpu threshold rising** n'est pas configurée, la valeur par défaut pour le niveau de seuil élevé est supérieure à 70 % et la valeur par défaut pour le niveau de seuil critique est supérieure à 95 %. La période de supervision par défaut est fixée à 1 minute.

Vous ne pouvez pas configurer le niveau de seuil critique du CPU, qui est maintenu à une valeur constante de 95 %. Les valeurs de seuil valides pour un seuil de CPU élevé sont comprises entre 10 et 94 %. Les valeurs valides pour la période de supervision sont comprises entre 1 et 60 minutes.

Configurer un seuil d'interface physique

Pour configurer le seuil d'interface physique, procédez comme suit :

Procédure

Configurez la valeur de seuil pour une interface physique SNMP.

snmp interface threshold *threshold_value*

Exemple :

```
ciscoasa(config)# snmp interface threshold 75%
```

Pour effacer la valeur de seuil d'une interface physique SNMP, utilisez la forme **no** de cette commande. La valeur de seuil est définie en pourcentage d'utilisation de la bande passante de l'interface. Les valeurs de seuil valides sont comprises entre 30 et 99 %. La valeur par défaut est 70 %.

La commande **snmp interface threshold** est disponible uniquement dans le contexte d'administration.

L'utilisation des interfaces physiques est supervisée en mode de contexte unique et multiple, et les interruptions pour les interfaces physiques dans le contexte système sont envoyées par l'entremise du contexte d'administration. Seules les interfaces physiques sont utilisées pour calculer l'utilisation du seuil.

Configurer les paramètres pour la version 1 ou 2c du SNMP

Pour configurer les paramètres pour la version 1 ou 2c du SNMP, procédez comme suit :

Procédure

Étape 1 Spécifiez le destinataire d'une notification SNMP, indiquez l'interface à partir de laquelle les interruptions sont envoyées et identifiez le nom et l'adresse IP du gestionnaire NMS ou SNMP qui peut se connecter à l'ASA.

snmp-server host{*interface hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1 2c**| *username*}] [**udp-port** *port*]

Exemple :

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2c
ciscoasa(config)# snmp-server host corp 172.18.154.159 community public

ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 2c
```

Le mot clé **trap** limite le NMS à la réception d'interruptions uniquement. Le mot clé **poll** limite le NMS à l'envoi de requêtes (interrogation) uniquement. Par défaut, les alertes SNMP sont activées. Par défaut, le port UDP est 162. L'identifiant de communauté est une clé secrète partagée entre l'ASA et le NMS. La clé est une valeur sensible à la casse pouvant comporter jusqu'à 32 caractères alphanumériques. Les espaces ne sont pas permises. L'identifiant de communauté par défaut est public. L'ASA utilise cette clé pour déterminer si la requête SNMP entrante est valide ou non. Par exemple, vous pouvez désigner un site avec un identifiant de communauté, puis configurer l'ASA et la station de gestion avec le même identifiant. L'ASA utilise l'identifiant spécifié et ne répond pas aux requêtes contenant un identifiant de communauté non valide. Cependant, si la supervision SNMP se fait par l'interface de gestion plutôt que par l'interface de diagnostic, l'interrogation a lieu sans que l'ASA ne valide l'identifiant de communauté. Après avoir utilisé un identifiant de communauté chiffré, seule la forme chiffrée est visible pour tous les systèmes (par exemple, interface de ligne de commande, ASDM, CSM, etc.). Le mot de passe en clair n'est pas visible. L'identifiant de communauté chiffré est toujours généré par l'ASA; vous devez généralement saisir la forme en clair.

Le mot clé **version** spécifie la version du SNMP à utiliser pour les interruptions et les requêtes (interrogation). La communication avec le serveur est autorisée uniquement en utilisant la version sélectionnée.

Pour recevoir des interruptions après avoir ajouté la commande **snmp-server host**, assurez-vous de configurer l'utilisateur sur le NMS avec les mêmes renseignements d'authentification que ceux configurés sur l'ASA.

Étape 2 Définissez l'identifiant de communauté, qui doit être utilisé *uniquement* avec la version 1 ou 2c du SNMP.

snmp-server community *community-string*

Exemple :

```
ciscoasa(config)# snmp-server community onceuponatime
```

Remarque
Vous devez éviter l'utilisation de caractères spéciaux (!, @, #, $, %, ^, &, *, \) dans les identifiants de communauté. En général, l'utilisation de caractères spéciaux réservés aux fonctions utilisées par le système d'exploitation peut entraîner des résultats inattendus. Par exemple, la barre oblique inverse (\) est interprétée comme un caractère d'échappement et ne doit pas être utilisée dans l'identifiant de communauté.

Étape 3 Définissez l'emplacement du serveur SNMP ou ses coordonnées.

snmp-server [**contact** | **location**] *text*

Exemple :

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

L'argument *text* spécifie le nom de la personne-ressource ou de l'administrateur système de l'ASA. Le nom est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.

Étape 4 Définissez le port d'écoute pour les requêtes SNMP.

snmp-server listen-port *lport*

Exemple :

```
ciscoasa(config)# snmp-server lport 192
```

L'argument *lport* est le port sur lequel les requêtes entrantes sont acceptées. Le port d'écoute par défaut est le 161. La commande **snmp-server listen-port** n'est disponible que dans le contexte d'administration et non pas dans le contexte système. Si vous configurez la commande **snmp-server listen-port** sur un port en cours d'utilisation, le message suivant apparaît :

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

Le fil SNMP existant continue d'interroger toutes les 60 secondes jusqu'à ce que le port soit disponible et émet le message de journal système %ASA-1-212001 si le port est toujours utilisé.

Configurer les paramètres pour la version 3 du SNMP

Pour configurer les paramètres pour la version 3 du SNMP, procédez comme suit :

Procédure

Étape 1 Spécifiez un nouveau groupe SNMP, qui doit être utilisé *uniquement* avec la version 3 du SNMP.

snmp-server group *group-name* **v3** [**auth** | **noauth** | **priv**]

Exemple :

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

Lorsqu'un identifiant de communauté est configuré, deux groupes supplémentaires dont le nom correspond à l'identifiant de communauté sont automatiquement générés : un pour le modèle de sécurité version 1 et un pour le modèle de sécurité version 2. Le mot clé **auth** active l'authentification des paquets. Le mot clé **noauth** indique qu'aucune authentification ou ni aucun chiffrement de paquet n'est utilisé. Le mot clé **priv** active le chiffrement et l'authentification des paquets. Aucune valeur par défaut n'existe pour les mots clés **auth** ou **priv**.

Étape 2 Configurez un nouvel utilisateur pour un groupe SNMP, qui doit être utilisé uniquement avec la version 3 du SNMP.

snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** {**sha** | **sha224** | **sha256** | **sha384**} *auth_password* [**priv** {**3des** | **aes** {**128** | **192** | **256**}} *priv_password*]]

Exemple :

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword
aes 128 mypassword
ciscoasa(config)# snmp-server user testuser1 public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

L'argument username est le nom de l'utilisateur sur l'hôte qui appartient à l'agent SNMP. Saisissez 32 caractères ou moins pour le nom d'utilisateur. Le nom doit commencer par une lettre. Les caractères valides sont les lettres, les chiffres, _ (trait de soulignement) et . (point), @ (at) et - (trait d'union).

L'argument group-name est le nom du groupe auquel appartient l'utilisateur. Le mot clé **v3** spécifie que le modèle de sécurité SNMP version 3 doit être utilisé et permet l'utilisation des mots clés **encrypted**, **priv** et **auth**. Le mot clé **engineID** est facultatif et spécifie l'ID du moteur de l'ASA qui a été utilisé pour localiser les renseignements d'authentification et de chiffrement de l'utilisateur. L'argument engineID doit spécifier un ID de moteur ASA valide.

Le mot clé **encrypted** spécifie le mot de passe au format chiffré. Les mots de passe cryptés doivent répondre aux exigences suivantes :

- Doit être au format hexadécimal.
- Doit contenir un minimum de 8 caractères et un maximum de 80 caractères.
- Doit contenir uniquement des lettres, des chiffres et les caractères suivants : ~`!@#%^&*()_-+{}[]|\:;"'<,>./
- Ne doit pas contenir les symboles suivants : $ (signe de dollar), ? (point d'interrogation) ou = (signe d'égalité).
- Doit contenir au moins cinq caractères différents.
- Ne doit pas contenir trop de chiffres ou de lettres consécutifs croissants ou décroissants. Par exemple, la chaîne « 12345 » comporte quatre caractères de ce type et la chaîne « ZYXW » en comporte trois. Si le nombre total de caractères de ce type dépasse une certaine limite (généralement plus de 4 à 6 occurrences), la vérification de la simplicité échouera.

  Remarque
  Le nombre de caractères consécutifs croissants ou décroissants n'est pas réinitialisé lorsque des caractères non croissants ou non décroissants sont utilisés entre eux. Par exemple, abcd&!21 échouera à la vérification du mot de passe, mais abcd&!25 n'échouera pas.

Le mot clé **auth** spécifie le niveau d'authentification (**sha**, **sha224**, **sha256** ou **sha384**) à utiliser. Le mot clé **priv** spécifie le niveau de chiffrement. Il n'existe aucune valeur par défaut pour les mots clés **auth** ou **priv**, ni aucun mot de passe par défaut.

Pour l'algorithme de chiffrement, vous pouvez spécifier le mot clé **3des** ou **aes**. Vous pouvez également spécifier la version de l'algorithme de chiffrement AES à utiliser : **128**, **192** ou **256**. L'argument auth-password spécifie le mot de passe d'authentification de l'utilisateur. L'argument priv-password spécifie le mot de passe de chiffrement de l'utilisateur.

Si vous ignorez un mot de passe, vous ne pouvez pas le récupérer et vous devez reconfigurer l'utilisateur. Vous pouvez spécifier un mot de passe en texte brut ou un condensé localisé. Le condensé localisé doit correspondre à l'algorithme d'authentification sélectionné pour l'utilisateur, qui peut être SHA, SHA-224, SHA-256, ou SHA-384. Lorsque la configuration de l'utilisateur s'affiche sur la console ou est écrite dans un fichier (par exemple, le fichier de configuration de démarrage), les condensés d'authentification et de confidentialité localisés s'affichent toujours au lieu d'un mot de passe en texte brut (voir le deuxième exemple).

La longueur minimum d'un mot de passe est de 1 caractère alphanumérique; cependant, nous vous conseillonns d'utiliser au moins 8 caractères alphanumériques pour des raisons de sécurité.

Lorsque vous utilisez SNMPv3 avec mise en grappe ou basculement, si vous ajoutez une nouvelle unité de grappe après la formation initiale de la grappe ou si vous remplacez une unité de basculement, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez rajouter les utilisateurs SNMPv3 à l'unité de contrôleou active pour forcer les utilisateurs à être dupliqués sur la nouvelle unité; ou vous pouvez ajouter les utilisateurs directement sur la nouvelle unité (les utilisateurs et les groupes SNMPv3 sont une exception à la règle selon laquelle vous ne pouvez pas saisir de commandes de configuration sur une unité de données en grappe). Reconfigurez chaque utilisateur en saisissant la commande **snmp-server user** *username group-name* **v3** sur l'unité de contrôle/active ou directement sur l'unité de données/secours avec les options *priv-password* et *auth-password* dans leur format non chiffré.

Si vous saisissez un utilisateur sur l'unité de contrôle/active avec le mot clé **encrypted**, un message d'erreur s'affiche pour vous informer que les commandes utilisateur SNMPv3 ne seront pas répliquées. Ce comportement signifie également que les commandes d'utilisateur et de groupe SNMPv3 existantes ne sont pas supprimées pendant la réplication.

Par exemple, une unité de contrôle/active utilisant des commandes saisies avec des clés chiffrées :

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a
priv aes 256 cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:
f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

Par exemple, une unité de données pendant la réplication de la grappe (apparaît uniquement si des commandes **snmp-server user** existent dans la configuration) :

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

Étape 3 Spécifiez le destinataire d'une notification SNMP. Indiquez l'interface à partir de laquelle les interruptions sont envoyées. Identifiez le nom et l'adresse IP du gestionnaire NMS ou SNMP qui peut se connecter à l'ASA.

snmp-server host *interface* {*hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

Exemple :

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1
ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 3 testuser3
```

Le mot clé **trap** limite le NMS à la réception d'interruptions uniquement. Le mot clé **poll** limite le NMS à l'envoi de requêtes (interrogation) uniquement. Par défaut, les alertes SNMP sont activées. Par défaut, le port UDP est 162. L'identifiant de communauté est une clé secrète partagée entre l'ASA et le NMS. La clé est une valeur sensible à la casse pouvant comporter jusqu'à 32 caractères alphanumériques. Les espaces ne sont pas permises. L'identifiant de communauté par défaut est public. L'ASA utilise cette clé pour déterminer si la requête SNMP entrante est valide. Par exemple, vous pouvez désigner un site avec un identifiant de communauté, puis configurer l'ASA et le NMS avec le même identifiant. L'ASA utilise l'identifiant spécifié et ne répond pas aux requêtes contenant un identifiant de communauté non valide. Après avoir utilisé un

identifiant de communauté chiffré, seule la forme chiffrée est visible pour tous les systèmes (par exemple, interface de ligne de commande, ASDM, CSM, etc.). Le mot de passe en clair n'est pas visible. L'identifiant de communauté chiffré est toujours généré par l'ASA; vous devez généralement saisir la forme en clair.

Le mot clé **version** spécifie la version du SNMP à utiliser pour les interruptions et les requêtes (interrogation). La communication avec le serveur est autorisée uniquement en utilisant la version sélectionnée.

Lorsque des hôtes SNMP version 3 sont configurés sur l'ASA, un utilisateur doit être associé à cet hôte.

Pour recevoir des interruptions après avoir ajouté la commande **snmp-server host**, assurez-vous de configurer l'utilisateur sur le NMS avec les mêmes renseignements d'authentification que ceux configurés sur l'ASA.

Étape 4 Définissez l'emplacement du serveur SNMP ou ses coordonnées.

snmp-server [**contact** | **location**] *text*

Exemple :

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

L'argument *text* spécifie le nom de la personne-ressource ou de l'administrateur système de l'ASA. Le nom est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.

Étape 5 Définissez le port d'écoute pour les requêtes SNMP.

snmp-server listen-port *lport*

Exemple :

```
ciscoasa(config)# snmp-server lport 192
```

L'argument *lport* est le port sur lequel les requêtes entrantes sont acceptées. Le port d'écoute par défaut est le 161. La commande **snmp-server listen-port** n'est disponible que dans le contexte d'administration et non pas dans le contexte système. Si vous configurez la commande **snmp-server listen-port** sur un port en cours d'utilisation, le message suivant apparaît :

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

Le fil SNMP existant continue d'interroger toutes les 60 secondes jusqu'à ce que le port soit disponible et émet le message de journal système %ASA-1-212001 si le port est toujours utilisé.

Configurer un groupe d'utilisateurs

Pour configurer une liste d'utilisateurs SNMP avec un groupe d'utilisateurs spécifiés, procédez comme suit :

Procédure

Configurez une liste d'utilisateurs SNMP.

snmp-server user-list *list_name* **username** *user_name*

Exemple :

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

L'argument *listname* spécifie le nom de la liste d'utilisateurs, qui peut comporter jusqu'à 33 caractères. La paire mot clé-argument **username** *user_name* spécifie les utilisateurs qui peuvent être configurés dans la liste des utilisateurs. Vous configurez les utilisateurs dans la liste des utilisateurs à l'aide de la commande **snmp-server user** *username*, qui est disponible uniquement si vous utilisez la version 3 de SNMP. La liste d'utilisateurs doit comporter plusieurs utilisateurs et peut être associée à un nom d'hôte ou à une plage d'adresses IP.

Associer les utilisateurs à un objet réseau

Pour associer un seul utilisateur ou un groupe d'utilisateurs d'une liste d'utilisateurs à un objet réseau, procédez comme suit :

Procédure

Associez un seul utilisateur ou un groupe d'utilisateurs dans une liste d'utilisateurs à un objet réseau.

snmp-server host-group *net_obj_name* [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

Exemple :

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

L'argument *net_obj_name* spécifie le nom de l'objet réseau de l'interface auquel un utilisateur ou un groupe d'utilisateurs est associé.

Le mot clé **trap** spécifie que seules des alertes peuvent être envoyées et que cet hôte n'est pas autorisé à naviguer (interrogation). Les alertes SNMP sont activées par défaut.

Le mot clé **poll** indique que l'hôte est autorisé à naviguer (interrogation), mais qu'aucune interruption ne peut être envoyée.

Le mot clé **community** spécifie qu'une chaîne autre que par défaut est requise pour les demandes du NMS ou lors de la génération des alertes envoyées au NMS. Vous pouvez utiliser ce mot clé uniquement pour la version 1 ou 2c du SNMP. L'argument *community-string* spécifie l'identifiant de communauté de type mot de passe qui est envoyé avec la notification ou dans une demande du NMS. L'identifiant de communauté peut comporter un maximum de 32 caractères.

Le mot clé **version** définit la version de notification SNMP à la version 1, 2c ou 3 à utiliser pour l'envoi d'interruptions et l'acceptation des demandes (interrogation). La version par défaut est 1.

L'argument *username* spécifie le nom de l'utilisateur si vous utilisez la version 3 du SNMP.

La paire mot de passe-argument **user-list** *list_name* spécifie le nom de la liste d'utilisateurs.

La paire mot de passe-argument **udp-port** *port* précise que les alertes SNMP doivent être envoyées à un hôte NMS sur un port autre que par défaut et définit le numéro de port UDP de l'hôte NMS. Le port UDP par défaut est 162.

Supervision SNMP

Consultez les commandes suivantes pour superviser SNMP.

- **show running-config snmp-server** [**default**]

  Cette commande affiche tous les renseignements de configuration du serveur SNMP.

- **show running-config snmp-server group**

  Cette commande affiche les paramètres de configuration du groupe SNMP.

- **show running-config snmp-server host**

  Cette commande affiche les paramètres de configuration utilisés par SNMP pour contrôler les messages et les notifications envoyés aux hôtes distants.

- **show running-config snmp-server host-group**

  Cette commande affiche les configurations du groupe d'hôtes SNMP.

- **show running-config snmp-server user**

  Cette commande affiche les paramètres de configuration SNMP basés sur l'utilisateur.

- **show running-config snmp-server user-list**

  Cette commande affiche les configurations de la liste d'utilisateurs SNMP.

- **show snmp-server engineid**

  Cette commande affiche l'ID du moteur SNMP configuré.

- **show snmp-server group**

  Cette commande affiche les noms des groupes SNMP configurés. Si l'identifiant de communauté a déjà été configuré, deux groupes supplémentaires s'affichent par défaut dans la sortie. Ce comportement est normal.

- **show snmp-server statistics**

  Cette commande affiche les caractéristiques configurées du serveur SNMP. Pour réinitialiser tous les compteurs SNMP à zéro, utilisez la commande **clear snmp-server statistics**.

- **show snmp-server user**

  Cette commande affiche les caractéristiques configurées des utilisateurs.

Exemples

L'exemple suivant montre comment afficher les statistiques du serveur SNMP :

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

L'exemple suivant montre comment afficher la configuration en cours d'exécution du serveur SNMP :

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

Exemples de SNMP

La section suivante fournit des exemples que vous pouvez utiliser comme référence pour toutes les versions de SNMP.

SNMP versions 1 et 2c

L'exemple suivant montre comment l'ASA peut recevoir des requêtes SNMP de l'hôte 192.0.2.5 sur l'interface interne, mais n'envoie aucune demande de journal système SNMP à aucun hôte :

```
ciscoasa(config)# snmp-server host 192.0.2.5
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
ciscoasa(config)# snmp-server community ohwhatakeyisthee
```

SNMP version 3

L'exemple suivant montre comment l'ASA peut recevoir des requêtes SNMP en utilisant le modèle de sécurité SNMP version 3, qui nécessite que la configuration suive cet ordre précis : groupe, suivi de l'utilisateur, suivi de l'hôte :

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

Historique de SNMP

Tableau 69 : Historique de SNMP

Nom de la caractéristique	Version	Description
SNMP versions 1 et 2c	7.0(1)	Fournit des renseignements sur la supervision du réseau ASA et les événements en transmettant les données entre le serveur SNMP et l'agent SNMP par l'identifiant de communauté en texte clair.
SNMP version 3	8.2(1)	Fournit un chiffrement et une prise en charge 3DES ou AES pour SNMP version 3, la forme la plus sécurisée des modèles de sécurité pris en charge. Cette version vous permet de configurer les utilisateurs, les groupes et les hôtes, ainsi que les caractéristiques d'authentification à l'aide d'USM. En outre, cette version permet le contrôle d'accès à l'agent et aux objets MIB et comprend une prise en charge MIB supplémentaire. Nous avons ajouté ou modifié les commandes suivantes : **show snmp-server engineid**, **show snmp-server group**, **show snmp-server user**, **snmp-server group**, **snmp-server user**, **snmp-server host**.
Chiffrement de mot de passe	8.3(1)	Prend en charge le chiffrement de mot de passe. Nous avons modifié les commandes suivantes : **snmp-server community**, **snmp-server host**.
Alertes SNMP et MIB	v 8.4(1)	Prend en charge les mots clés supplémentaires suivants : **connection-limit-reached**, **cpu threshold rising**, **entity cpu-temperature**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. Le tableau entPhysicalTable signale les entrées pour les capteurs, les ventilateurs, les alimentations et les composants connexes. Prend en charge les MIB supplémentaires suivantes : CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, DISMAN-EVENT-MIB, DISMAN-EXPRESSION-MIB, ENTITY-SENSOR-MIB, NAT-MIB. Prend en charge les interruptions supplémentaires suivantes : ceSensorExtThresholdNotification, clrResourceLimitReached, cpmCPURisingThreshold, mteTriggerFired, natPacketDiscard, warmStart. Nous avons introduit ou modifié les commandes suivantes : **snmp cpu threshold rising**, **snmp interface threshold**, **snmp-server enable traps**.
Prise en charge de l'OID IF-MIB ifAlias	8.2(5)/8.4(2)	L'ASA prend désormais en charge l'OID ifAlias. Lorsque vous parcourez l'IF-MIB, l'OID ifAlias sera défini à la valeur qui a été définie pour la description de l'interface.

Nom de la caractéristique	Version	Description
Module de services ASA (ASASM)	8.5(1)	L'ASASM prend en charge toutes les MIB et interruptions présentes dans 8.4(1), à l'exception des éléments suivants : MIB non prises en charge dans 8.5(1) : • CISCO-ENTITY-SENSOR-EXT-MIB (seuls les objets du groupe entPhySensorTable sont pris en charge). • ENTITY-SENSOR-MIB (seuls les objets du groupe entPhySensorTable sont pris en charge). • DISMAN-EXRPSION-MIB (seuls les objets des groupes expExpressionTable, expObjectTable et expValueTable sont pris en charge). Interruptions non prises en charge dans 8.5(1) : • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB). Cette interruption est utilisée uniquement pour les défaillances d'alimentation, les défaillances de ventilateur et les événements de température élevée du processeur. • InterfacesBandwidthUtilization.
Interruptions SNMP	8.6(1)	Prend en charge les mots clés supplémentaires suivants pour les modèles ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X : **entity power-supply-presence**, **entity power-supply-failure**, **entity chassis-temperature**, **entity chassis-fan-failure, entity power-supply-temperature**. Nous avons modifié la commande suivante : **snmp-server enable traps**.
MIB liées au VPN	9.0(1)	Une version mise à jour de CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB a été implementée pour prendre en charge la fonctionnalité de chiffrement de nouvelle génération. Les MIB suivantes ont été activées pour l'ASASM : • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
MIB TrustSec de Cisco	9.0(1)	La prise en charge de la MIB suivante a été ajoutée : CISCO-TRUSTSEC-SXP-MIB.

Nom de la caractéristique	Version	Description
OID SNMP	9.1(1)	Cinq nouveaux OID de type prestataire physique SNMP ont été ajoutés pour prendre en charge les appareils ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X.
MIB NAT	9.1(2)	Ajout des OID cnatAddrBindNumberOfEntries et cnatAddrBindSessionCount pour prendre en charge les entrées xlate_count et max_xlate_count, qui sont équivalents à l'autorisation de l'interrogation à l'aide de la commande **show xlate count**.
Hôtes SNMP, groupes d'hôtes et listes d'utilisateurs	9.1(5)	Vous pouvez maintenant ajouter jusqu'à 4 000 hôtes. Le nombre de destinations d'interrogation actives prises en charge est de 128. Vous pouvez spécifier un objet réseau pour indiquer les hôtes individuels que vous souhaitez ajouter en tant que groupe d'hôtes. Vous pouvez associer plusieurs utilisateurs à un hôte. Nous avons introduit ou modifié les commandes suivantes : **snmp-server host-group**, **snmp-server user-list**, **show running-config snmp-server**, **clear configure snmp-server**.
Taille des messages SNMP	9.2(1)	La limite de taille des messages que SNMP envoie a été augmentée à 1 472 octets.
OID et MIB SNMP	9.2(1)	L'ASA prend désormais en charge l'OID cpmCPUTotal5minRev. L'ASA virtuel a été ajouté en tant que nouveau produit aux OID sysObjectID et entPhysicalVendorType de SNMP. Les fichiers CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB ont été mis à jour pour prendre en charge la nouvelle plateforme ASA virtuel. Une nouvelle MIB SNMP pour superviser l'utilisation des licences partagées des VPN a été ajoutée.
OID et MIB SNMP	9.3(1)	La prise en charge de CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) a été ajoutée pour l'ASASM.

Nom de la caractéristique	Version	Description
MIB et alertes SNMP	9.3(2)	Les fichiers CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB ont été mis à jour pour prendre en charge l'ASA 5506-X. L'ASA 5506-X a été ajouté en tant que nouveau produit aux tableaux d'OID sysObjectID et entPhysicalVendorType de SNMP. L'ASA prend désormais en charge CISCO-CONFIG-MAN-MIB, qui vous permet de faire les opérations suivantes : • Savoir quelles commandes ont été saisies pour une configuration en particulier. • Avertir le NMS lorsqu'une modification s'est produite dans la configuration d'exécution. • Suivez les horodatages associés à la dernière fois que la configuration d'exécution a été modifiée ou enregistrée. • Suivez les autres modifications apportées aux commandes, comme les détails du terminal et les sources de commandes. Nous avons modifié la commande suivante : **snmp-server enable traps**.
MIB et alertes SNMP	9.4(1)	Les ASA 5506W-X, ASA 5506H-X, ASA 5508-X et ASA 5516-X ont été ajoutés en tant que nouveaux produits aux tableaux d'OID sysObjectID et entPhysicalVendorType de SNMP.
Hôtes d'interruption de serveur SNMP illimités par contexte	9.4(1)	L'ASA prend en charge un nombre illimité d'hôtes d'interruption de serveur SNMP par contexte. La sortie de la commande **show snmp-server host** affiche uniquement les hôtes actifs qui interrogent l'ASA, ainsi que les hôtes configurés de manière statique. Nous avons modifié la commande suivante : **show snmp-server host**.
Ajout de la prise en charge pour ISA 3000	9.4(1.225)	La gamme de produits ISA 3000 est désormais prise en charge pour SNMP. Nous avons ajouté de nouveaux OID pour cette plateforme. La commande **snmp-server enable traps entity** a été modifiée pour inclure une nouvelle variable *l1-bypass-status*. Cela active le changement d'état du contournement matériel. Nous avons modifié la commande suivante : **snmp-server enable traps entity**.
Prise en charge de cempMemPoolTable dans CISCO-ENHANCED-MEMPOOL-MIB	9.6(1)	Le tableau cempMemPoolTable de CISCO-ENHANCED-MEMPOOL-MIB est maintenant pris en charge. Il s'agit d'un tableau des entrées de surveillance de la réserve de mémoire pour toutes les entités physiques d'un système géré. **Remarque** CISCO-ENHANCED-MEMPOOL-MIB utilise des compteurs de 64 bits et prend en charge les rapports de mémoire sur les plateformes avec plus de 4 Go de RAM.

Nom de la caractéristique	Version	Description
Prise en charge des MIB en mode d'horloge E2E transparent pour le protocole PTP (Precision Time Protocol)	9.7(1)	Les MIB correspondant au mode d'horloge E2E transparent sont maintenant prises en charge. **Remarque** Seules les opérations SNMP get, bulkget, getnext et walk sont prises en charge.
SNMP sur IPv6	9.9(2)	L'ASA prend désormais en charge SNMP sur IPv6, y compris la communication avec des serveurs SNMP sur IPv6, permettant l'exécution de requêtes et d'interruptions sur IPv6 et prenant en charge les adresses IPv6 pour les MIB existantes. Nous avons ajouté les nouveaux objets MIB IPv6 SNMP suivants, comme décrit dans la RFC 8096. • ipv6InterfaceTable (OID : 1.3.6.1.2.1.4.30) : contient des renseignements spécifiques à IPv6 par interface. • ipAddressPrefixTable (OID :1.3.6.1.2.1.4.32) : comprend tous les préfixes appris par cette entité. • ipAddressTable (OID : 1.3.6.1.2.1.4.34) : contient des renseignements d'adressage pertinents pour les interfaces de l'entité. • ipNetToPhysicalTable (OID : 1.3.6.1.2.1.4.35) : contient le mappage des adresses IP aux adresses physiques. Commande nouvelle ou modifiée : **snmp-server host** **Remarque** La commande **snmp-server host-group** ne prend pas en charge IPv6.
Prise en charge de l'activation et de la désactivation des résultats de la mémoire libre et des statistiques de mémoire utilisée lors des opérations de marche SNMP	9.10(1)	Pour éviter la surutilisation des ressources du processeur, vous pouvez activer et désactiver la requête de mémoire libre et les statistiques de mémoire utilisée collectées par les opérations de marche de SNMP. Commande nouvelle ou modifiée : **snmp-server enable oid**
Prise en charge de l'activation et de la désactivation des résultats de la mémoire libre et des statistiques de mémoire utilisée lors des opérations de marche SNMP	9.12(1)	Pour éviter la surutilisation des ressources du processeur, vous pouvez activer et désactiver la requête de mémoire libre et les statistiques de mémoire utilisée collectées par les opérations de marche de SNMP. Nous n'avons pas modifié de commandes.
Authentification SNMPv3	9.14(1)	Vous pouvez maintenant utiliser le code HMAC SHA-256 pour l'authentification de l'utilisateur. Commandes nouvelles ou modifiées : **snmp-server user**
Pour les paires de basculements en version 9.14(1) ou toute version ultérieure, l'ASA ne partage plus les données du moteur client SNMP avec son homologue.	9.14(1)	L'ASA ne partage plus les données du moteur client SNMP avec son homologue.

Nom de la caractéristique	Version	Description
Interrogation SNMP sur le VPN de site à site	9.14(2)	Pour une interrogation SNMP sécurisée sur un VPN de site à site, incluez l'adresse IP de l'interface externe dans la liste d'accès de la carte cryptographique dans le cadre de la configuration du VPN.
La prise en charge des OID CISCO-MEMORY-POOL-MIB est rendue obsolète	9.15(1)	Les OID CISCO-MEMORY-POOL-MIB (ciscoMemoryPoolUsed, ciscoMemoryPoolFree) sont obsolètes pour les systèmes qui utilisent des compteurs de 64 bits. Le tableau cempMemPoolTable de CISCO-ENHANCED-MEMPOOL-MIB fournit des entrées de supervision de la réserve de mémoire pour les systèmes qui utilisent des compteurs de 64 bits.
Authentification SNMPv3	9.16(1)	Vous pouvez maintenant utiliser SHA-224 et SHA-384 pour l'authentification de l'utilisateur. Vous ne pouvez plus utiliser MD5 pour l'authentification de l'utilisateur. Vous ne pouvez plus utiliser DES pour le chiffrement. Commandes nouvelles ou modifiées : **snmp-server user**
SNMP sur IPv6	9.17(1)	La commande **snmp-server host-group** prend désormais en charge les objets d'hôte, de plage et de sous-réseau IPv6.
Prise en charge de l'interface de boucle avec retour pour SNMP	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour SNMP. Commandes nouvelles/modifiées : **interface loopback**, **snmp-server host**



CHAPITRE 49

Données de télémétrie et du Cisco Success Network

Ce chapitre décrit le Cisco Success Network et comment l'activer sur l'ASA. Il répertorie également les points de données télémétriques qui sont envoyés au nuage Security Service Engine (SSE).

- À propos de Cisco Success Network , à la page 1495
- Activer ou désactiver Cisco Success Network , à la page 1496
- Afficher les données de télémétrie d'ASA , à la page 1497
- Cisco Success Network – Données de télémétrie, à la page 1498
- Déboguer les données de télémétrie, à la page 1504

À propos de Cisco Success Network

Cisco Success Network est un service en nuage activé par l'utilisateur qui établit une connexion sécurisée avec le nuage Security Service Exchange (SSE) afin de diffuser en continu les renseignements et les statistiques d'utilisation de l'ASA. La télémétrie en continu fournit un mécanisme permettant de transmettre l'utilisation de l'ASA et d'autres détails dans un format structuré (JSON) à des stations de gestion à distance, ce qui présente les avantages suivants :

- Pour vous informer des services de soutien technique supplémentaires et de la supervision offerte pour votre produit.
- Pour aider Cisco à améliorer ses produits.

Par défaut, Cisco Success Network est activé sur les plateformes Firepower 4100/9300 qui hébergent les périphériques ASA (au niveau de la lame). Cependant, pour que les données de télémétrie soient transmises, vous devez activer la configuration sur FXOS au niveau du châssis (consultez le Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS) ou activez le Cisco Success Network sur le gestionnaire de châssis (consultez le Guide de configuration du Firepower Chassis Manager de Cisco Firepower Cisco Firepower 4100/9300 FXOS). L'ASA vous permet de désactiver le service de télémétrie à tout moment.

Les données de télémétrie collectées sur vos périphériques ASA comprennent l'utilisation du processeur, de la mémoire, du disque, de la bande passante et des licences, la liste des fonctionnalités configurées, les renseignements sur la grappe et le basculement, etc. Veuillez vous référer à Cisco Success Network – Données de télémétrie, à la page 1498.

Plateformes prises en charge et configurations requises

- Pris en charge sur les plateformes FP9300/4100 avec l'ASA version 9.13.1 ou supérieure.
- Nécessite FXOS version 2.7.1 ou ultérieure pour la connexion au nuage.
- Le connecteur SSE sur FXOS doit être connecté au nuage SSE. Cette connexion est établie par l'activation et l'enregistrement de la licence Smart avec le système dorsal de licence Smart. Le connecteur SSE sur FXOS est automatiquement enregistré dans le nuage SSE lors de l'enregistrement de la licence Smart.
- La configuration de Cisco Success Network doit être activée sur le gestionnaire de châssis.
- La configuration de télémétrie doit être activée sur l'ASA.

Comment les données de télémétrie ASA atteignent le nuage SSE

Cisco Success Network est pris en charge sur les plateformes Firepower 4100/9300 dans l'ASA 9.13(1) par défaut. Le gestionnaire de service FXOS envoie quotidiennement des requêtes de télémétrie à l'application ASA en cours d'exécution sur la plateforme. Le moteur ASA, en fonction de l'état de configuration et de connectivité, envoie les données de télémétrie en mode autonome ou en mode grappe à FXOS. En d'autres termes, si la prise en charge de la télémétrie est activée dans l'ASA et que le connecteur SSE est connecté, le fil de télémétrie extrait les renseignements nécessaires de diverses sources telles que les API de système, de plateforme ou d'appareil, les API de licence, les API de CPU, les API de mémoire, les API de disque, les API de la fonction Smart Call Home, etc. Cependant, si la prise en charge de la télémétrie est désactivée dans l'ASA ou que le connecteur SSE est déconnecté, l'ASA envoie une réponse à FXOS (appAgent) indiquant l'état de la configuration de la télémétrie et n'envoie aucune donnée de télémétrie.

FXOS n'a qu'une seule instance de connecteur SSE en cours d'exécution. Lorsqu'il est enregistré auprès du nuage SSE, il est considéré comme un seul périphérique et l'infrastructure SSE attribue à FXOS un ID de périphérique. Tout rapport de télémétrie envoyé par le biais du connecteur SSE est classé sous le même ID de périphérique. Par conséquent, FXOS regroupe les rapports de télémétrie de chaque ASA en un seul rapport. D'autres contenus, tels que les renseignements sur le compte de licence Smart, sont ajoutés au rapport. FXOS envoie ensuite le rapport final au nuage SSE. Les données de télémétrie sont enregistrées dans l'échange de données SSE (DX) et sont disponibles pour l'équipe informatique de Cisco.

Activer ou désactiver Cisco Success Network

Avant de commencer

- Activez et enregistrez la licence Smart sur FXOS.
- Activez la prise en charge de la télémétrie sur FXOS au niveau du châssis (consultez le Guide de configuration de l'interface de ligne de commande de Cisco Firepower 4100/9300 FXOS) ou activez le Cisco Success Network sur le gestionnaire de châssis (consultez le Guide de configuration du Firepower Chassis Manager de Cisco Firepower 4100/9300 FXOS).

Procédure

Pour activer le service de télémétrie sur l'ASA, dans le mode de configuration globale, saisissez la commande suivante. Utilisez la forme no (non) de la commande pour désactiver le service de télémétrie :

[**no**] **service telemetry**

Exemple :

```
ciscoasa(config)# service telemetry
ciscoasa(config)# no service telemetry
```

Prochaine étape

- Vous pouvez afficher la configuration et le journal des activités de télémétrie ou les données de télémétrie. Voir la section Afficher les données de télémétrie d'ASA , à la page 1497.
- Pour afficher un exemple de données de télémétrie et de champs de données, consultez Cisco Success Network – Données de télémétrie, à la page 1498

Afficher les données de télémétrie d'ASA

Avant de commencer

- Activez le service de télémétrie sur l'ASA. Voir la section Activer ou désactiver Cisco Success Network , à la page 1496.

Procédure

Pour afficher les données de télémétrie sur les périphériques ASA de votre réseau, saisissez la commande suivante en mode d'exécution privilégié :

show telemetry [**history | last-report | sample**]

Exemple :

```
ciscoasa# show telemetry history
17:38:24 PDT Apr 30 2019: Telemetry support on the blade: enabled
17:38:03 PDT Apr 30 2019: Telemetry support on the blade: disabled
11:49:47 PDT Apr 29 2019: msgId 3. Telemetry support on the chassis: disabled
11:48:47 PDT Apr 29 2019: msgId 2. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent
11:47:47 PDT Apr 29 2019: msgId 1. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent.
```

Utilisez **history** pour afficher les 100 derniers événements liés à la configuration et aux activités de télémétrie; **last-report** pour afficher les dernières données de télémétrie envoyées à FXOS au format JSON, et **sample** pour afficher les données de télémétrie générées instantanément au format JSON.

Cisco Success Network – Données de télémétrie

Cisco Success Network est pris en charge sur les plateformes Firepower 4100/9300 par défaut. Le gestionnaire de service FXOS envoie quotidiennement des requêtes de télémétrie au moteur ASA en cours d'exécution sur la plateforme. Le moteur ASA, en cas de réception de la demande, en fonction de l'état de la connectivité, envoie les données de télémétrie en mode autonome ou en mode grappe à FXOS. Les tableaux suivants fournissent des renseignements sur les points de données de télémétrie, leur description et des exemples de valeurs.

Tableau 70 : Renseignements sur le périphérique

Point de données	Description	Exemple de valeur
Modèle du périphérique	le modèle d'appareil (Device model)	Appareils de sécurité adaptatifs de Cisco
Serial Number (numéro de série)	Numéro de série de l'appareil	FCH183771EZ
Heure système	Disponibilité du système	11658000
Observations	Matériel	FPR9K-SM-24
Mode de déploiement	Type de déploiement	Natif
Mode de contexte de sécurité	Unique/Multiple	Unique

Tableau 71 : Renseignements sur les versions

Point de données	Description	Exemple de valeur
Variable globale de version	Version d'ASA	9.13.1.5
Version de gestionnaire d'appareil	Version de gestionnaire d'appareil	7.10.1

Tableau 72 : Renseignements de licence

Point de données	Description	Exemple de valeur
Variable globale de la licence Smart	Licences activées	regid.2015-01.com.cisco.ASA - SSP-STRONG-ENCRYPTION, 1.0_555507e9-85f8-4e41-96de-860b59f10bbe

Tableau 73 : Renseignements sur la plateforme

Point de données	Description	Exemple de valeur
UC	Utilisation du CPU au cours des 5 dernières minutes	fiveSecondsPercentage : 0.2000000, oneMinutePercentage : 0, fiveMinutesPercentage : 0
Mémoire	Utilisation de la mémoire	freeMemoryInBytes : 225854966384, usedMemoryInBytes : 17798281616, totalMemoryInBytes : 243653248000
Disque	Utilisation du disque	freeGB : 21.237285, usedGB : 0.238805, totalGB : 21.476090
Bande passante	Utilisation de la bande passante	receivedPktsPerSec : 3, receivedBytesPerSec : 212, transmittedPktsPerSec : 3, transmittedBytesPerSec : 399

Tableau 74 : Renseignements sur les fonctionnalités

Point de données	Description	Exemple de valeur
Liste des fonctionnalités	Liste des fonctionnalités activées	nom : grappe état : activé

Tableau 75 : Renseignements sur la grappe

Point de données	Description	Exemple de valeur
Renseignements sur la grappe	Renseignements sur la grappe	clusterGroupName : ssp-cluster interfaceMode : spanned unitName : unit-3-3 unitState : SLAVE otherMembers : items : memberName : unit-2-1 memberState : MASTER memberSerialNum : FCH183771BA

Tableau 76 : Renseignements sur le basculement

Point de données	Description	Exemple de valeur
Basculement	Renseignements sur le basculement	myRole : Primary, peerRole : Secondary, myState : active, peerState : standby, peerSerialNum : FCH183770EZ

Tableau 77 : Renseignements de connexion

Point de données	Description	Exemple de valeur
Ouvrir une session	Historique de connexion	loginTimes : 2 fois dans les 2 derniers jours, lastSuccessfulLogin : 12:25:36 (HAP) 11 mars 2019

Exemple de données de télémétrie ASA

Voici un exemple des données de télémétrie envoyées par l'ASA au format JSON. Lorsque le gestionnaire de service reçoit cette entrée, il regroupe les données de tous les ASA et ajoute les en-têtes et les champs nécessaires avant de les envoyer au connecteur SSE. Les en-têtes/champs comprennent « version », « metadata », « payload » avec « recordedAt », « recordType », « recordVersion » et des données de télémétrie ASA, « smartLicenseProductInstanceIdentifier », « smartLicenseVirtualAccountName », etc.

```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
```

```
    "contentType": "application/json"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1557363423705,
    "SSP": {
      "SSPdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "JMX2235L01J",
        "smartLicenseProductInstanceIdentifier": "f85a5bb0-xxxx-xxxx-xxxx-xxxxxxxxx",
        "smartLicenseVirtualAccountName": "SSP-general",
        "systemUptime": 198599,
        "udiProductIdentifier": "FPR-C9300-AC"
      },
      "versions": {
        "items": [
          {
            "type": "package_version",
            "version": "92.7(1.342g)"
          }
        ]
      }
    },
    "asaDevices": {
      "items": [
        {
    "deviceInfo": {
        "deviceModel": "Cisco Adaptive Security Appliance",
        "serialNumber": "AANNNXXX",
        "systemUptime": 285,
        "udiProductIdentifier": "FPR9K-SM-36",
        "deploymentType": "Native",
        "securityContextMode": "Single"
    },
    "versions": {
        "items": [
            {
                "type": "asa_version",
                "version": "201.4(1)82"
            },
            {
                "type": "device_mgr_version",
                "version": "7.12(1)44"
            }
        ]
    },
    "licenseActivated": {
        "items": [
            {
                "type": "Strong encryption",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-STRONG-ENCRYPTION,1.0_xxxxxxx-xxxx-xxxx-96de-860b59f10bbe",

                "count": 1
            },
            {
                "type": "Carrier",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-MOBILE-SP,1.0_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
                "count": 1
            }
        ]
    },
```

```
"CPUUsage": {
    "fiveSecondsPercentage": 0,
    "oneMinutePercentage": 0,
    "fiveMinutesPercentage": 0
},
"memoryUsage": {
    "freeMemoryInBytes": 99545662064,
    "usedMemoryInBytes": 20545378704,
    "totalMemoryInBytes": 120091040768
},
"diskUsage": {
    "freeGB": 21.237027,
    "usedGB": 0.239063,
    "totalGB": 21.476090
},
"bandwidthUsage": {
    "receivedPktsPerSec": 3,
    "receivedBytesPerSec": 268,
    "transmittedPktsPerSec": 4,
    "transmittedBytesPerSec": 461
},
"featureStatus": {
    "items": [
        {
            "name": "call-home",
            "status": "enabled"
        },
        {
            "name": "cluster",
            "status": "enabled"
        },
        {
            "name": "firewall_user_authentication",
            "status": "enabled"
        },
        {
            "name": "inspection-dns",
            "status": "enabled"
        },
        {
            "name": "inspection-esmtp",
            "status": "enabled"
        },
        {
            "name": "inspection-ftp",
            "status": "enabled"
        },
        {
            "name": "inspection-netbios",
            "status": "enabled"
        },
        {
            "name": "inspection-rsh",
            "status": "enabled"
        },
        {
            "name": "inspection-sip",
            "status": "enabled"
        },
        {
            "name": "inspection-sqlnet",
            "status": "enabled"
        },
        {
```

```
                "name": "inspection-sunrpc",
                "status": "enabled"
            },
            {
                "name": "inspection-tftp",
                "status": "enabled"
            },
            {
                "name": "inspection-xdmcp",
                "status": "enabled"
            },
            {
                "name": "logging-console",
                "status": "informational"
            },
            {
                "name": "management-mode",
                "status": "normal"
            },
            {
                "name": "sctp-engine",
                "status": "enabled"
            },
            {
                "name": "threat_detection_basic_threat",
                "status": "enabled"
            },
            {
                "name": "threat_detection_stat_access_list",
                "status": "enabled"
            },
            {
                "name": "webvpn-activex-relay",
                "status": "enabled"
            },
            {
                "name": "webvpn-dtls",
                "status": "enabled"
            }
        ]
    },
    "clusterInfo": {
        "clusterGroupName": "ssp-cluster",
        "interfaceMode": "spanned",
        "unitName": "unit-3-3",
        "unitState": "SLAVE",
        "otherMembers": {
            "items": [
                {
                    "memberName": "unit-2-1",
                    "memberState": "MASTER",
                    "memberSerialNum": "FCH183771BA"
                },
                {
                    "memberName": "unit-2-3",
                    "memberState": "SLAVE",
                    "memberSerialNum": "FLM1949C6JR"
                },
                {
                    "memberName": "unit-2-2",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                },
                {
```

```
                    "memberName": "unit-3-2",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                },
                {
                    "memberName": "unit-3-1",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                }
            ]
        }
    },
    "loginHistory": {
        "loginTimes": "1 times in last 1 days",
        "lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019"
    }
}
```

Déboguer les données de télémétrie

Avant de commencer

- Activez le service de télémétrie sur l'ASA. Voir la section Activer ou désactiver Cisco Success Network , à la page 1496.

Procédure

Étape 1 Pour afficher les messages de débogage liés à la télémétrie, activez le service de débogage de télémétrie à l'aide de la commande suivante en mode d'exécution privilégié :

debug telemetry *<1-255>*

Exemple :

```
asa# debug telemetry ?
   <1-255>  Specify an optional debug level (default is 1)
```

Utilisez la forme **no** de la commande pour désactiver le service de débogage de la télémétrie.

Étape 2 Pour afficher les messages de télémétrie de débogage pour le niveau de débogage sélectionné, utilisez la commande suivante :

show debug telemetry

Exemple :

```
asa# show debug telemetry
debug telemetry  enabled at level 1

[telemetry_collect_device_info]: telemetry successfully collected device info
[telemetry_collect_versions]: telemetry successfully collected version info
[telemetry_collect_licenses]: no smart-lic entitlement in use
[telemetry_collect_cpu]: telemetry successfully collected cpu info
[telemetry_collect_memory]: telemetry successfully collected mem info
[telemetry_collect_disk_usage]: telemetry successfully collected disk info
[telemetry_collect_bandwidth_usage]: telemetry successfully collected bandwidth usage info
[telemetry_collect_enabled_feature_status]: telemetry successfully collected enabled feature
```

```
 info
[telemetry_collect_cluster_info]: telemetry successfully collected cluster info
[telemetry_collect_failover_info]: ha is not configured
[telemetry_get_user_login_hist]: telemetry successfully collected login history
[telemetry_collect_blocks]: telemetry successfully collected block info
[telemetry_collect_perfmon]: telemetry successfully collected perfmon stats
[telemetry_collect_resource_usage]: telemetry successfully collected res usage
[telemetry_collect_process_cpu_usage]: telemetry successfully collected res usage
[telemetry_collect_crashinfo]: telemetry successfully collected crashinfo
[telemetry_collect]: the serialized string is generated
[telemetry_collect]: successfully allocated mem for serialized string
[telemetry_history_add_record]: telemetry has a new history record: 16:23:29 PDT Oct 22
2019: Telemetry support on the blade: enabled
[telemetry_history_add_record]: telemetry has a new history record: 16:24:01 PDT Oct 22
2019: Telemetry support on the blade: disabled
```



CHAPITRE 50

Alarmes pour Cisco ISA 3000

Ce chapitre donne un aperçu du système d'alarme dans l'ISA 3000 et décrit également comment configurer et superviser les alarmes.

- À propos des alarmes, à la page 1507
- Valeurs par défaut pour les alarmes, à la page 1509
- Configurer les alarmes, à la page 1509
- Surveillance des alarmes, à la page 1512
- Historique des alarmes, à la page 1515

À propos des alarmes

Vous pouvez configurer l'ISA 3000 pour qu'il émette des alarmes dans diverses conditions. Si les conditions ne correspondent pas aux paramètres configurés, le système déclenche une alarme, qui est signalée par des DEL, des messages du journal système, des déroutements SNMP et par des périphériques externes connectés à l'interface de sortie d'alarme. Par défaut, les alarmes déclenchées n'émettent que des messages syslog.

Vous pouvez configurer le système d'alarme pour surveiller les éléments suivants :

- Bloc d'alimentation
- Capteurs de température principal et secondaire.
- Interfaces d'entrée d'alarme.

L'ISA 3000 est doté de capteurs internes ainsi que de deux interfaces d'entrée d'alarme et d'une interface de sortie d'alarme. Vous pouvez connecter des capteurs externes, comme des capteurs de porte, aux entrées d'alarme. Vous pouvez connecter des périphériques d'alarme externes, comme des avertisseurs sonores ou des voyants, à l'interface de sortie d'alarme.

L'interface de sortie d'alarme est un mécanisme de relais. Selon les conditions d'alarme, le relais est soit activé ou désactivé. Lorsqu'elle est sous tension, tout périphérique connecté à l'interface est activé. Un relais hors tension entraîne l'état inactif de tous les périphériques connectés. Le relais reste activé tant que des alarmes sont déclenchées.

Pour en savoir plus sur la connexion des capteurs externes et du relais d'alarme, consulter le Guide d'installation du matériel du périphérique de sécurité industrielle Cisco ISA 3000.

Interfaces d'entrée d'alarme

Vous pouvez connecter les interfaces d'entrée (ou contacts) d'entrée d'alarme à des capteurs externes, par exemple celui qui détecte si une porte est ouverte.

Chaque interface d'entrée d'alarme a un voyant DEL correspondant. Ces voyants DEL transmettent l'état d'alarme de chaque entrée d'alarme. Vous pouvez configurer le déclencheur et la gravité de chaque entrée d'alarme. En plus du voyant DEL, vous pouvez configurer le contact pour déclencher le relais de sortie (pour activer une alarme externe), pour envoyer des messages syslog et pour envoyer des déroutements SNMP.

Le tableau suivant explique les états des voyants DEL en réponse aux conditions d'alarme pour les entrées d'alarme. Il explique également le comportement du relais de sortie, des messages du journal système et des interruptions SNMP, si vous activez ces réponses pour l'entrée d'alarme.

État de l'alarme	DEL	Relais de sortie	Syslog	Interruptions SNMP
Alarme non configurée	Désactivé	—	—	—
Aucune alarme déclenchée	Vert fixe	—	—	—
Alarme activée	Alarme mineure : rouge fixe Alarme majeure : rouge clignotant	Relais sous tension	Journal système généré	Déroutement SNMP envoyé.
Fin d'alarme	Vert fixe	Relais désactivé	Journal système généré	—

Interface de sortie d'alarme

Vous pouvez connecter une alarme externe, comme un avertisseur ou un voyant, à l'interface de sortie d'alarme.

L'interface de sortie d'alarme fonctionne comme un relais et est également dotée d'un voyant DEL correspondant, qui transmet l'état d'alarme d'un capteur externe connecté à l'interface d'entrée et des capteurs internes tels que la double alimentation et les capteurs de température. Vous configurez les alarmes qui doivent activer le relais de sortie, le cas échéant.

Le tableau suivant explique les états des DEL et du relais de sortie en réponse à des conditions d'alarme. Elle explique également le comportement des messages syslog et des alertes SNMP si vous activez ces réponses à l'alarme.

État de l'alarme	DEL	Relais de sortie	Syslog	Interruptions SNMP
Alarme non configurée	Désactivé	—	—	—
Aucune alarme déclenchée	Vert fixe	—	—	—
Alarme activée	Rouge fixe	Relais sous tension	Journal système généré	Déroutement SNMP envoyé.

État de l'alarme	DEL	Relais de sortie	Syslog	Interruptions SNMP
Fin d'alarme	Vert fixe	Relais désactivé	Journal système généré	—

Valeurs par défaut pour les alarmes

Le tableau suivant précise les valeurs par défaut pour les interfaces d'entrée d'alarme (contacts), l'alimentation redondante et la température.

	Alerte	initiales	Gravité	Interruptions SNMP	Relais de sortie	Messages de journalisation du système (syslog)
Contact d'alarme 1	Activé	État fermé	Mineur	Désactivé	Désactivé	Activé
Contact d'alarme 2	Activé	État fermé	Mineur	Désactivé	Désactivé	Activé
Alimentation redondante (si activée)	Activé	—	—	Désactivé	Désactivé	Activé
Température	Activé pour l'alarme de température principale (valeurs par défaut de 92 °C et de -40 °C pour les seuils respectivement) Désactivé pour l'alarme secondaire.	—	—	Activé pour l'alarme de température principale	Activé pour l'alarme de température principale	Activé pour l'alarme de température principale

Configurer les alarmes

Pour configurer des alarmes pour ISA 3000, procédez comme suit.

Procédure

Étape 1 Configurez la gravité d'un ou de tous les contacts d'alarme.

alarm contact {*contact_number* | **all**} **severity {major | minor | none}**

Exemple :

```
ciscoasa(config)# alarm contact 1 severity major
```

Saisissez un numéro de contact (**1** ou **2**) ou saisissez **all** (tout) pour configurer toutes les alarmes. Saisissez **major** (majeure), **minor** (mineure) ou **none** (aucune) comme gravité. La valeur par défaut est : mineure.

Étape 2 Configurez les déclencheurs d'un ou de tous les contacts d'alarme.

alarm contact {*contact_number* | **all**} **trigger {closed | open}**

Si vous spécifiez **open** (ouvert), une alarme se déclenchera lorsqu'un contact normalement fermé (connectivité électrique normale) est ouvert ou lorsque le courant cesse de circuler.

Si vous spécifiez **closed** (fermé), une alarme se déclenchera lorsque le contact normalement ouvert (pas de connectivité électrique) est fermé ou lorsque le courant commence à circuler.

Par exemple, si un capteur de porte est connecté à une entrée d'alarme, son état normalement ouvert n'a pas de courant électrique circulant à travers les contacts. Si la porte est ouverte, le courant électrique circule à travers les contacts, activant l'alarme.

Exemple :

```
ciscoasa(config)# alarm contact 1 trigger open
```

Saisissez un numéro de contact (**1** ou **2**) ou saisissez **all** (tout) pour configurer toutes les alarmes. Entrez **open** (ouvert) ou **closed** (fermé) pour spécifier le déclencheur. La valeur par défaut est closed (fermé).

Étape 3 Activez le relais, la journalisation du système et les alertes SNMP pour les contacts d'alarme.

Lorsque le relais est activé et qu'une condition d'alarme se produit, le relais est activé et l'appareil relié au relais est activé. Lorsque le relais est activé, le voyant DEL d'alarme est rouge fixe.

- Activez le relais pour l'alarme d'entrée.

alarm facility input-alarm *contact_number* **relay**

Exemple :

```
ciscoasa(config)# alarm facility input-alarm 1 relay
```

Saisissez un numéro de contact (**1** ou **2**). Par défaut, le relais pour les entrées d'alarme est désactivé.

- Activez la journalisation du système.

alarm facility input-alarm *contact_number* **syslog**

Exemple :

```
ciscoasa(config)# alarm facility input-alarm 1 syslog
```

Saisissez un numéro de contact (**1** ou **2**).

- Activez les alertes SNMP.

alarm facility input-alarm *contact_number* **notifies**

Exemple :

```
ciscoasa(config)# alarm facility input-alarm 1 notifies
```

Saisissez un numéro de contact (**1** ou **2**).

Étape 4 (Facultatif) Entrez une description pour les contacts d'alarme d'entrée.

alarm contact *contact_number* | **description** *string*

Exemple :

```
ciscoasa(config)# alarm contact 1 description Door_Open
```

Le contact_number spécifie le contact d'alarme pour lequel la description est configurée. La description peut comporter jusqu'à 80 caractères alphanumérique et sera incluse dans les messages du journal système.

Pour définir la description par défaut du numéro de contact correspondant, utilisez la commande **no alarm contact contact_number description**.

Étape 5 Configurez les alarmes d'alimentation.

Remarque
L'alimentation redondante doit être activée pour que les alarmes d'alimentation fonctionnent.

Consultez les commandes suivantes pour la configuration des alarmes d'alimentation :

- **power-supply dual**

  Cette commande active la double alimentation.

- **alarm facility power-supply rps disable**

  Cette commande désactive l'alarme d'alimentation. Dans son état par défaut, cette alarme est désactivée. Si l'alarme est activée, utilisez cette commande pour la désactiver.

- **alarm facility power-supply rps notifies**

  Cette commande envoie des interruptions d'alarme d'alimentation à un serveur SNMP.

- **alarm facility power-supply rps relay**

  Cette commande associe l'alarme d'alimentation au relais.

- **alarm facility power-supply rps syslog**

  Cette commande envoie des interruptions d'alarme d'alimentation à un serveur de journal système.

Étape 6 Configurez les seuils de température.

alarm facility temperature {**primary | secondary**} {**high | low**} *threshold*

Exemple :

```
ciscoasa(config)# alarm facility temperature primary high 90
ciscoasa(config)# alarm facility temperature primary low 40
ciscoasa(config)# alarm facility temperature secondary high 85
ciscoasa(config)# alarm facility temperature primary low 35
```

Pour l'alarme de température principale, les valeurs de seuil valides sont comprises entre -40 °C et 92 °C. Pour l'alarme de température secondaire, les valeurs de seuil valides sont comprises entre -35 °C et 85 °C. Si un seuil de température est configuré pour l'alarme secondaire, seule l'alarme secondaire sera activée.

Utilisez la forme **no** (non) de chaque commande pour désactiver ou rétablir les valeurs par défaut. L'utilisation de la forme **no** (non) des commandes pour l'alarme principale ne désactivera pas l'alarme et rétablira les valeurs par défaut de 92 °C pour le seuil élevé et de -40 °C pour le seuil bas. L'utilisation de la forme **no** (non) de la commande pour l'alarme secondaire la désactivera.

Étape 7 Activez les alertes SNMP, le relais et la journalisation du système pour les alarmes de température.

Consultez les commandes suivantes pour activer le relais, les alertes SNMP et les journaux système pour les alarmes de température :

- **alarm facility temperature** {**primary | secondary**} **notifies**

  Cette commande envoie des interruptions d'alarme de température principale ou secondaire à un serveur SNMP.

- **alarm facility temperature** {**primary | secondary**} **relay**

  Cette commande associe l'alarme de température principale ou secondaire au relais.

- **alarm facility temperature** {**primary | secondary**} **syslog**

  Cette commande envoie des interruptions d'alarme de température principale ou secondaire à un serveur de journal système.

Utilisez la forme no (non) de chaque commande pour désactiver le relais, les alertes SNMP et les journaux système.

Surveillance des alarmes

Consultez les commandes suivantes pour superviser les alarmes :

Procédure

- **show alarm settings**

  Cette commande affiche tous les paramètres d'alarme globaux.

```
ciscoasa> show alarm settings
Power Supply
         Alarm                   Disabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Temperature-Primary
         Alarm                   Enabled
         Thresholds           MAX: 92C                MIN: -40C
         Relay                   Enabled
         Notifies                Enabled
         Syslog                  Enabled
Temperature-Secondary
         Alarm                   Disabled
         Threshold
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Input-Alarm 1
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
Input-Alarm 2
         Alarm                   Enabled
```

```
        Relay                  Disabled
        Notifies               Disabled
        Syslog                 Enabled
```

- **show environment alarm-contact**

  Cette commande affiche tous les paramètres d'alarme externe.

```
ciscoasa> show environment alarm-contact
ALARM CONTACT 1
   Status:       not asserted
   Description:  external alarm contact 1
   Severity:     minor
   Trigger:      closed
ALARM CONTACT 2
   Status:       not asserted
   Description:  external alarm contact 2
   Severity:     minor
   Trigger:      closed
```

- **show facility-alarm status** [**info** | **major** | **minor**]

  Cette commande affiche toutes les alarmes en fonction de la gravité spécifiée.

  La sortie affiche les renseignements suivants :

Colonne	Description
Source	Périphérique à partir duquel l'alarme a été déclenchée. Il s'agit généralement du nom d'hôte configuré sur le périphérique.
Gravité	Majeure ou mineure
Description	Type d'alarme déclenchée. Par exemple, la température, le contact externe, l'alimentation redondante, etc.
Relais	Sous tension ou hors tension
Durée	Horodatage de l'alarme déclenchée

```
ciscoasa> show facility-alarm status info
Source      Severity    Description                                   Relay
        Time
ciscoasa   minor        external alarm contact 1 triggered  Energized         06:56:50
 UTC Mon Sep 22 2014
ciscoasa   minor        Temp below Secondary Threshold De-energized           06:56:49
 UTC Mon Sep 22 2014
ciscoasa   major       Redundant pwr missing or failed    De-energized        07:00:19
 UTC Mon Sep 22 2014
ciscoasa   major        Redundant pwr missing or failed    De-energized       07:00:19
 UTC Mon Sep 22 2014

ciscoasa> show facility-alarm status major
Source      Severity    Description                                   Relay
        Time
ciscoasa    major       Redundant pwr missing or failed    De-energized     07:00:19
UTC Mon Sep 22 2014
ciscoasa   major        Redundant pwr missing or failed    De-energized     07:00:19
UTC Mon Sep 22 2014
```

```
ciscoasa> show facility-alarm status minor
Source      Severity    Description                                   Relay
        Time
ciscoasa   minor        external alarm contact 1 triggered  Energized         06:56:50
 UTC Mon Sep 22 2014
ciscoasa   minor        Temp below Secondary Threshold De-energized     06:56:49 UTC
Mon Sep 22 2014
```

- **show facility-alarm relay**

  Cette commande affiche tous les relais sous tension.

```
ciscoasa> show facility-alarm relay
Source      Severity    Description                                   Relay
        Time
ciscoasa   minor        external alarm contact 1 triggered  Energized         06:56:50
 UTC Mon Sep 22 2014
```

Historique des alarmes

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge des ports d'alarme pour l'ISA 3000	9.7(1)	L'ISA 3000 prend désormais en charge deux broches d'entrée d'alarme et une broche de sortie d'alarme, avec des voyants DEL pour indiquer l'état des alarmes. Des capteurs externes peuvent être connectés aux entrées d'alarme. Un relais matériel externe peut être connecté à la broche de sortie d'alarme. Vous pouvez configurer les descriptions des alarmes externes. Vous pouvez également indiquer la gravité et le déclencheur pour les alarmes externes et internes. Toutes les alarmes peuvent être configurées pour le relais, la supervision et la journalisation. Nous avons introduit les commandes suivantes : **alarm contact description, alarm contact severity, alarm contact trigger, alarm facility input-alarm, alarm facility power-supply rps, alarm facility temperature, alarm facility temperature high, alarm facility temperature low, clear configure alarm, clear facility-alarm output, show alarm settings, show environment alarm-contact**. Nous avons introduit les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Alarm Port (Port d'alarme)** > **Alarm Contact (Contact d'alarme)** **Configuration** > **Device Management (Gestion des périphériques)** > **Alarm Port (Port d'alarme)** > **Redundant Power Supply (Bloc d'alimentation redondant)** **Configuration** > **Device Management (Gestion des périphériques)** > **Alarm Port (Port d'alarme)** > **Temperature (Température)** **Monitoring (Supervision)** > **Properties (Propriétés)** > **Alarm (Alarme)** > **Alarm Settings (Paramètres d'alarme)** **Monitoring (Supervision)** > **Properties (Propriétés)** > **Alarm (Alarme)** > **Alarm Contact (Contact d'alarme)** **Monitoring (Supervision)** > **Properties (Propriétés)** > **Alarm (Alarme)** > **Facility Alarm Status (État d'alarme de l'installation)**



CHAPITRE 51

Rapports anonymes et Smart Call Home

Ce chapitre décrit comment configurer les services de création de rapports anonymes et les services Smart Call Home.

- À propos des rapports anonymes, à la page 1517
- À propos de Smart Call Home, à la page 1518
- Lignes directrices relatives aux rapports anonymes et à Smart Call Home, à la page 1524
- Configurer les rapports anonymes et Smart Call Home, à la page 1525
- Supervision des rapports anonymes et de Smart Call Home, à la page 1537
- Exemples de Smart Call Home, à la page 1538
- Historique des rapports anonymes et de Smart Call Home, à la page 1539

À propos des rapports anonymes

Vous pouvez contribuer à l'amélioration de la plateforme ASA en activant les rapports anonymes, qui permettent à Cisco de recevoir en toute sécurité un minimum de renseignements sur les erreurs et l'intégrité de l'appareil. Si vous activez la fonctionnalité, votre identité de client restera anonyme et aucune information d'identification ne sera envoyée.

L'activation de la création de rapports anonymes crée un point de confiance et installe un certificat. Un certificat CA est requis pour que votre ASA valide le certificat de serveur présent sur le serveur Web Smart Call Home et pour former la session HTTPS afin que votre ASA puisse envoyer des messages en toute sécurité. Cisco importe un certificat prédéfini dans le logiciel. Si vous décidez d'activer les rapports anonymes, un certificat est installé sur l'ASA avec un nom de point de confiance codé en dur : _SmartCallHome_ServerCA. Lorsque vous activez la création de rapports anonymes, ce point de confiance est créé, le certificat approprié est installé et vous recevez un message au sujet de cette action. Le certificat apparaît ensuite dans votre configuration.

Si le certificat approprié existe déjà dans votre configuration lorsque vous activez les rapports anonymes, aucun point de confiance n'est créé et aucun certificat n'est installé.

Remarque Lorsque vous activez les rapports anonymes, vous acceptez de transférer les données spécifiées à Cisco ou aux fournisseurs agissant pour le compte de Cisco (y compris dans des pays en dehors des États-Unis). Cisco protège la confidentialité de tous ses clients. Pour en savoir plus sur le traitement des renseignements personnels par Cisco, consultez la Déclaration de confidentialité de Cisco à l'adresse suivante : http://www.cisco.com/web/siteassets/legal/privacy.html

Lorsque l'ASA configure les rapports anonymes de Smart Call Home en arrière-plan, l'ASA crée automatiquement un point de confiance contenant le certificat de la CA qui émet le certificat de serveur Call Home. L'ASA prend désormais en charge la validation du certificat si la hiérarchie d'émission du certificat de serveur change, sans avoir besoin de l'intervention du client pour apporter des modifications à la hiérarchie des certificats. Vous pouvez également importer automatiquement les certificats du groupe de confiance afin que l'ASA renouvelle la hiérarchie des certificats sans intervention manuelle.

Lorsque vous mettez à niveau ASA 9.14(2.14), la configuration du point de confiance passe automatiquement de CallHome_ServerCA à CallHome_ServerCA2.

Exigence DNS

Un serveur DNS doit être configuré correctement pour que l'ASA atteigne le serveur Cisco Smart Call Home et envoie des messages à Cisco. Comme il est possible que l'ASA réside dans un réseau privé et n'ait pas accès au réseau public, Cisco vérifie votre configuration DNS puis la configure pour vous, au besoin, en procédant comme suit :

1. Effectuer une recherche DNS pour tous les serveurs DNS configurés.
2. Obtenir le serveur DNS à partir du serveur DHCP en envoyant des messages DHCPINFORM sur l'interface du niveau de sécurité le plus élevé.
3. Utiliser les serveurs DNS de Cisco pour la recherche.
4. Utiliser des adresses IP statiques de façon aléatoire pour tools.cisco.com.

Ces tâches sont effectuées sans modifier la configuration actuelle. (Par exemple, le serveur DNS appris à partir du DHCP ne sera pas ajouté à la configuration.)

Si aucun serveur DNS n'est configuré et que l'ASA ne peut pas atteindre le serveur Cisco Smart Call Home, Cisco génère un message de journal système avec le niveau de gravité d'avertissement pour chaque message Smart Call Home envoyé pour vous rappeler de configurer le DNS correctement.

Consultez le guide des messages de journal système pour obtenir des renseignements sur les messages de journal système.

À propos de Smart Call Home

Une fois entièrement configuré, Smart Call Home détecte les problèmes sur votre site et les signale à Cisco ou par l'intermédiaire d'autres canaux définis par l'utilisateur (comme la messagerie électronique ou directement), souvent avant même que vous ne soyez conscient de l'existence de ces problèmes. Selon la gravité de ces problèmes, Cisco répond à vos problèmes de configuration système, à vos annonces de fin de vie de produit, à vos problèmes d'avis de sécurité, etc. en fournissant les services suivants :

- Identification rapide des problèmes grâce à une surveillance continue, des alertes proactives en temps réel et des diagnostics détaillés.
- Signalement des problèmes potentiels grâce aux notifications Smart Call Home, dans lesquelles une demande de service a été ouverte, avec toutes les données de diagnostic jointes.
- Résolution plus rapide des problèmes critiques grâce à un accès direct et automatique aux experts du TAC de Cisco.
- Utilisation plus efficace des ressources en personnel grâce à une résolution de problèmes plus rapide.
- Génération automatique des demandes de service auprès du TAC de Cisco (si vous disposez d'un contrat de service), acheminées vers l'équipe d'assistance appropriée, qui fournit des renseignements détaillés à propos du diagnostic permettant d'accélérer la résolution des problèmes.

Le portail Smart Call Home offre un accès rapide aux renseignements requis qui vous permettent d'effectuer les opérations suivantes :

- Passer en revue tous les messages, les diagnostics et les recommandations de Smart Call Home en un seul endroit.
- Vérifier l'état des demandes de service.
- Consulter les renseignements les plus récents sur l'inventaire et la configuration de tous les appareils compatibles avec Smart Call Home.

S'abonner aux groupes d'alertes

Un groupe d'alertes est un sous-ensemble prédéfini des alertes Smart Call Home prises en charge par l'ASA. Les différents types d'alertes Smart Call Home sont regroupés dans différents groupes d'alertes, selon leur type. Chaque groupe d'alertes signale la sortie de certaines interfaces de ligne de commande. Les groupes d'alertes Smart Call Home pris en charge sont les suivants :

- syslog
- diagnostic
- environnement
- stocks
- configuration
- menace
- snapshot
- télémétrie
- test

Attributs des groupes d'alertes

Les groupes d'alertes ont les attributs suivants :

- Les événements s'enregistrent d'abord auprès d'un groupe d'alertes.

- Un groupe peut s'associer à plusieurs événements.
- Vous pouvez vous abonner à des groupes d'alertes spécifiques.
- Vous pouvez activer et désactiver des groupes d'alertes spécifiques. Le paramètre par défaut est activé pour tous les groupes d'alertes.
- Les groupes d'alertes de diagnostic et d'environnement prennent en charge l'abonnement aux messages périodiques.
- Le groupe d'alertes de journal système prend en charge l'abonnement basé sur l'ID de message.
- Vous pouvez configurer un seuil pour l'utilisation du CPU et de la mémoire pour le groupe d'alertes d'environnement. Lorsqu'un paramètre donné a dépassé un seuil prédéfini, un message est envoyé. La plupart des valeurs de seuil dépendent de la plateforme et ne peuvent pas être modifiées.
- Vous configurez le groupe d'alertes d'instantané pour envoyer la sortie des interfaces de ligne de commande que vous spécifiez.

Messages envoyés à Cisco par des groupes d'alertes

Les messages sont envoyés à Cisco périodiquement et chaque fois que l'ASA se recharge. Ces messages sont classés par groupes d'alertes.

Les alertes d'inventaire comprennent la sortie des commandes suivantes :

- **show version** : affiche la version du logiciel ASA, la configuration matérielle, la clé de licence et les données de disponibilité associées pour le périphérique.
- **show inventory—**Récupère et affiche les renseignements d'inventaire sur chaque produit Cisco installé dans l'appareil réseau. Chaque produit est identifié par des renseignements d'appareil uniques, appelés UDI, qui est une combinaison de trois éléments de données distincts : l'identifiant de produit (PID), l'identifiant de version (VID) et le numéro de série (SN).
- **show failover state** : affiche l'état de basculement des deux unités d'une paire de basculement. Les renseignements affichés comprennent l'état principal ou secondaire de l'unité, l'état actif/veille de l'unité et le dernier motif signalé pour le basculement.
- **show environment** : affiche des renseignements sur l'environnement système pour les composants du système ASA, tels que l'état opérationnel du matériel pour le châssis, les pilotes, les ventilateurs et les alimentations, ainsi que l'état de la température, la tension et l'utilisation du processeur.

Les alertes de configuration comprennent la sortie des commandes suivantes :

- **show context** : affiche les interfaces allouées et l'URL du fichier de configuration, le nombre de contextes configurés, ou si vous activez la création de rapports anonymes dans l'espace d'exécution du système, à partir d'une liste de tous les contextes.
- **show call-home registered-module status** : affiche l'état du module enregistré. Si vous utilisez le mode de configuration système, la commande affiche l'état du module de système en fonction de l'ensemble du périphérique, et non en fonction du contexte.
- **show running-config** : affiche la configuration en cours d'exécution sur l'ASA.
- **show startup-config** : affiche la configuration de démarrage.

- **show access-list | include elements** : affiche les compteurs d'accès et une valeur d'horodatage pour une liste d'accès.

Les alertes de diagnostic comprennent la sortie des commandes suivantes :

- **show failover** : affiche des renseignements sur l'état de basculement de l'unité.
- **show interface : affiche des statistiques sur l'interface.**
- **show cluster info : affiche des renseignements sur la grappe.**
- **show cluster history : affiche l'historique de la grappe.**
- **show crashinfo** (tronqué) : après un rechargement inattendu du logiciel, le périphérique envoie un fichier d'information sur les plantages modifié qui ne contient que la section de recherche de la source du fichier. Ainsi, seuls les appels de fonction, les valeurs de registre et les vidages de pile sont signalés à Cisco.
- **show tech-support no-config : affiche les renseignements utilisés pour le diagnostic par les analystes de l'assistance technique.**

Les alertes d'environnement comprennent la sortie des commandes suivantes :

- **show environment** : affiche des renseignements sur l'environnement système pour les composants du système ASA, tels que l'état opérationnel du matériel pour le châssis, les pilotes, les ventilateurs et les alimentations, ainsi que l'état de la température, la tension et l'utilisation du processeur.
- **show cpu usage** : affiche les renseignements sur l'utilisation du processeur.
- **show memory detail** : affiche les détails de la mémoire système libre et allouée.

Les alertes de menace comprennent la sortie des commandes suivantes :

- **show threat-detection rate** : affiche les statistiques de détection des menaces.
- **show threat-detection shun** : affiche les hôtes actuellement banis.
- **show shun** : affiche les renseignements sur le bannissement.
- **show dynamic-filter reports top** : génère des rapports sur les 10 principaux sites malveillants, ports et hôtes infectés classés par le filtre de réseau de zombies.

Les alertes d'instantané peuvent comprendre la sortie des commandes suivantes :

- **show conn count** : affiche le nombre de connexions actives.
- **show asp drop** : affiche le chemin de sécurité accéléré des paquets ou des connexions abandonnés.

Les alertes de télémétrie comprennent la sortie des commandes suivantes :

- **show perfmon detail : affiche** les détails de performance de l'ASA.
- **show traffic – affiche l'activité de transmission et de réception de l'interface.**
- **show conn count** : affiche le nombre de connexions actives.
- **show vpn-sessiondb summary : affiche les renseignements sur le résumé de la session VPN.**
- **show vpn load-balancing : affiche les statistiques de durée d'exécution pour la configuration de la grappe virtuelle d'équilibrage de charges VPN.**

- **show local-host | include interface : affiche les états du réseau des hôtes locaux.**
- **show memory : affiche un résumé de la mémoire physique maximum et de la mémoire libre actuelle disponible pour le système d'exploitation.**
- **show context** : affiche les interfaces allouées et l'URL du fichier de configuration, le nombre de contextes configurés, ou si vous activez la création de rapports anonymes dans l'espace d'exécution du système, à partir d'une liste de tous les contextes.
- **show access-list | include elements** : affiche les compteurs d'accès et une valeur d'horodatage pour une liste d'accès.
- **show interface : affiche des statistiques sur l'interface.**
- **show threat-detection statistics protocol : affiche les statistiques du protocole IP.**
- **show phone-proxy media-sessions count : affiche le nombre de sessions multimédias correspondantes stockées par le mandataire téléphonique.**
- **show phone-proxy secure-phones count : affiche le nombre de téléphones capables de fonctionner en mode sécurisé stockés dans la base de données.**
- **show route : affiche la table de routage.**
- **show xlate count : affiche le nombre de sessions NAT (xlates).**

Seuil de gravité des messages

Lorsque vous abonnez un profil de destination à certains groupes d'alertes, vous pouvez définir un seuil pour l'envoi des messages de groupe d'alertes en fonction du niveau de gravité des messages. Tout message dont la valeur est inférieure au seuil spécifié du profil de destination n'est pas envoyé à la destination.

Le tableau suivant affiche le mappage entre les niveaux de gravité des messages et les niveaux de gravité du journal système.

Tableau 78 : Mappage des niveaux de gravité des messages et des niveaux du journal système

Niveau	Niveau de gravité des messages	Niveau de gravité du journal système	Description
9	Catastrophique	S. O.	Défaillance catastrophique à l'échelle du réseau.
8	Sinistre	S. O.	Incidence importante sur le réseau.
7	Déterminé par le mot clé de l'interface de ligne de commande spécifié : **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	0	Urgence. Système inutilisable.

Niveau	Niveau de gravité des messages	Niveau de gravité du journal système	Description
6	Déterminé par le mot clé de l'interface de ligne de commande spécifié : **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	1	Alerte. Conditions critiques; une attention immédiate est requise.
5	Déterminé par le mot clé de l'interface de ligne de commande spécifié : **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	2	Critique. Conditions majeures.
4	Déterminé par le mot clé de l'interface de ligne de commande spécifié : **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	3	Erreur. Conditions mineures.
3	Avertissement	4	Conditions de mise en garde.
2	Notification	5	Notification de base et messages d'information. Peuvent être sans importance pris isolément.
1	Normal	6	de l'autre partie. Événement normal, indiquant un retour à l'état normal.
0	Débogage	7	Messages de débogage (paramètre par défaut).

Profils d'abonnement

Un profil d'abonnement vous permet d'associer les destinataires cibles aux groupes concernés. Lorsqu'un événement enregistré auprès d'un groupe abonné dans un profil se déclenche, le message associé à l'événement est envoyé aux destinataires configurés. Les profils d'abonnement possèdent les attributs suivants :

- Vous pouvez créer et configurer plusieurs profils.
- Un profil peut configurer plusieurs destinataires de courriel ou HTTPS.
- Un profil peut abonner plusieurs groupes à un niveau de gravité spécifié.
- Un profil prend en charge trois formats de message : texte court, texte long et XML.
- Vous pouvez activer et désactiver un profil spécifique. Les profils sont désactivés par défaut.
- Vous pouvez préciser la taille maximum des messages. La valeur par défaut est de 3 Mo.

Un profil par défaut, « Cisco TAC », a été fourni. Le profil par défaut comporte un ensemble prédéfini de groupes (de diagnostic, d'environnement, d'inventaire, de configuration et de télémétrie) pour superviser et prédéfinir les courriels de destination et les URL HTTPS. Le profil par défaut est créé automatiquement lorsque vous configurez Smart Call Home pour la première fois. L'adresse courriel de destination est callhome@cisco.com et l'URL de destination est https://tools.cisco.com/its/service/oddce/services/DDCEService.

Remarque Vous ne pouvez pas modifier l'adresse courriel de destination ni l'URL de destination du profil par défaut.

Lorsque vous abonnez un profil de destination aux groupes d'alertes de configuration, d'inventaire, de télémétrie ou d'instantané, vous pouvez choisir de recevoir les messages du groupe d'alertes de manière asynchrone ou périodique à une heure spécifiée.

Le tableau suivant mappe le groupe d'alertes par défaut à son abonnement au niveau de gravité et à sa période (le cas échéant) :

Tableau 79 : Mappage d'abonnement entre le groupe d'alertes et le niveau de gravité

Groupe d'alertes	Niveau de gravité	Période
Configuration	Information	Mensuelle
Diagnostic	Informatif et supérieur	S. O.
Environnement	Notification et supérieur	S. O.
Inventaire	Information	Mensuelle
Snapshot	Information	s.o.
Syslog	Journal système équivalent	S. O.
Télémétrie	Information	Tous les jours
Tester	s.o.	s.o.
La chasse aux menaces	Notification	s.o.

Lignes directrices relatives aux rapports anonymes et à Smart Call Home

Cette section comprend des lignes directrices et des limites que vous devez consulter avant de configurer les rapports anonymes et Smart Call Home.

Lignes directrices relatives aux rapports anonymes

- Le DNS doit être configuré.
- Si un message de rapport anonyme ne peut pas être envoyé lors du premier essai, l'ASA réessaie deux fois avant d'abandonner le message.

- Les rapports anonymes peuvent coexister avec d'autres configurations de Smart Call Home sans modifier la configuration existante. Par exemple, si Smart Call Home est désactivé avant d'activer la création de rapports anonymes, il reste désactivé, même après l'activation des rapports anonymes.
- Si les rapports anonymes sont activés, vous ne pouvez pas supprimer le point de confiance, et lorsque les rapports anonymes sont désactivés, le point de confiance reste. Si les rapports anonymes sont désactivés, vous pouvez supprimer le point de confiance, mais la désactivation des rapports anonymes n'entraînera pas la suppression du point de confiance.
- Si vous utilisez une configuration en mode de contexte multiple, les commandes **dns**, **interface** et **trustpoint** sont dans le contexte d'administration et les commandes **call-home** sont dans le contexte système.
- Vous pouvez automatiser la mise à jour de l'ensemble de groupes de confiance à des intervalles périodiques afin que Smart Call Home puisse rester actif si le certificat autosigné du serveur CA change. Cette fonctionnalité de renouvellement automatique des groupes de confiance n'est pas prise en charge dans le cadre des déploiements à contextes multiples.

Lignes directrices relatives à Smart Call Home

- En mode de contexte multiple, la commande subscribe-to-alert-group snapshot periodic est divisée en deux commandes : l'une pour obtenir des renseignements de la configuration système et l'autre pour obtenir des renseignements du contexte utilisateur.
- Le serveur dorsal Smart Call Home n'accepte que les messages au format XML.
- Un message Smart Call Home est envoyé à Cisco pour signaler des événements de grappe importants si vous avez activé la mise en grappe et configuré Smart Call Home pour vous abonner au groupe d'alertes de diagnostic avec un niveau de gravité critique. Un message de mise en grappe Smart Call Home est envoyé uniquement pour les événements suivants :
  - Lorsqu'une unité rejoint la grappe
  - Lorsqu'une unité quitte la grappe
  - Lorsqu'une unité de grappe devient l'unité de contrôle de grappe
  - Lorsqu'une unité secondaire tombe en panne dans la grappe

  Chaque message envoyé comprend les renseignements suivants :
  - Le nombre de membres actifs dans la grappe
  - La sortie de la commande **show cluster info** et de la commande **show cluster history** sur l'unité de contrôle de grappe

Configurer les rapports anonymes et Smart Call Home

Les rapports anonymes font partie du service Smart Call Home et permettent à Cisco de recevoir de manière anonyme un minimum de renseignements sur les erreurs et l'intégrité de votre appareil, mais le service Smart Call Home offre une assistance personnalisée sur l'intégrité de votre système, ce qui permet au TAC de Cisco de superviser vos appareils et d'ouvrir un dossier lorsqu'il y a un problème, souvent avant même que vous sachiez que le problème est survenu.

Vous pouvez avoir les deux services configurés sur votre système en même temps, bien que la configuration du service Smart Call Home offre les mêmes fonctionnalités que les rapports anonymes, ainsi que des services personnalisés.

Lorsque vous passez en mode de configuration, vous recevez une invite qui vous demande d'activer les services de création de rapports anonymes et de Smart Call Home en fonction des lignes directrices suivantes :

- À l'invite, vous pouvez choisir [Y]es (Oui), [N]o (Non) ou [A]sk later (Demander plus tard). Si vous choisissez [A]sk later (Demander plus tard), vous recevrez un rappel à nouveau dans sept jours ou lors du rechargement de l'ASA. Si vous continuez à choisir [A]sk later (Demander plus tard), l'ASA répond deux fois de plus à des intervalles de sept jours avant de prendre en charge une réponse [N]o (Non) et ne demande plus de réponse.
- Si vous n'avez pas reçu d'invite, vous pouvez activer la création de rapports anonymes ou Smart Call Home en effectuant les étapes dans Configurer les rapports anonymes, à la page 1526 ou dans Configurer Smart Call Home, à la page 1527.

Configurer les rapports anonymes

Pour configurer les rapports anonymes, procédez comme suit.

Procédure

Étape 1 Activez la fonctionnalité Rapports anonymes et créez un nouveau profil anonyme.

call-home reporting anonymous

Exemple :

```
ciscoasa(config)# call-home reporting anonymous
```

La saisie de cette commande crée un point de confiance et installe un certificat utilisé pour vérifier l'identité du serveur Web Cisco.

Étape 2 (Facultatif) Assurez-vous que vous disposez d'une connexion au serveur et que votre système peut envoyer des messages.

call-home test reporting anonymous

Exemple :

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...

INFO: Succeeded
```

Un message de réussite ou d'erreur renvoie les résultats du test.

Configurer Smart Call Home

La configuration du service Smart Call Home sur votre ASA comprend les tâches suivantes :

Procédure

Étape 1 Activez le service Smart Call Home. Consultez Activer Smart Call Home, à la page 1527.

Étape 2 Configurez le serveur de messagerie par lequel les messages Smart Call Home sont envoyés aux abonnés. Consultez Configurer le serveur de messagerie, à la page 1532.

Étape 3 Configurez les coordonnées pour les messages Smart Call Home. Consultez Configurer les coordonnées du client, à la page 1530.

Étape 4 Définissez les paramètres de traitement des alertes, tels que le taux maximum d'événements qui peuvent être gérés. Consultez Configurer l'abonnement des groupes d'alertes, à la page 1529.

Étape 5 Configurez les profils d'abonnement aux alertes. Consultez Configurer un profil de destination, à la page 1534.

Chaque profil d'abonnement aux alertes identifie les éléments suivants :

- Les abonnés à qui les messages Smart Call Home sont envoyés, comme un serveur Smart Call Home chez Cisco ou une liste de destinataires de courriels.
- Catégories d'informations pour lesquelles vous souhaitez recevoir des alertes, comme les informations de configuration ou d'inventaire.

Activer Smart Call Home

Pour activer Smart Call Home et activer votre profil call-home, procédez comme suit :

Procédure

Étape 1 Activez le service Smart Call Home.

service call-home

Exemple :

```
ciscoasa(config)# service call-home
```

Étape 2 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call home
```

Déclarer et authentifier le point de confiance d'une autorité de certification

Si Smart Call Home est configuré pour envoyer des messages à un serveur web par HTTPS, vous devez configurer l'ASA pour faire confiance au certificat du serveur web ou au certificat de l'autorité de certification (CA) qui a émis le certificat. Le certificat de serveur Cisco Smart Call Home Production est émis par Verisign. Le certificat de serveur Cisco Smart Call Home Staging est émis par Digital Signature Trust Company.



Remarque Vous devez définir le point de confiance pour aucun type de client/aucune utilisation de validation afin d'empêcher son utilisation pour la validation VPN.

Pour déclarer et authentifier le certificat de sécurité du serveur Cisco et établir la communication avec le serveur HTTPS de Cisco pour le service Smart Call Home, procédez comme suit :

Procédure

Étape 1 (Mode de contexte multiple seulement) Installez le certificat dans le contexte d'administration.

changeto context *admincontext*

Exemple :

```
ciscoasa(config)# changeto context contextA
```

Étape 2 Configurez un point de confiance et préparez l'inscription du certificat.

crypto ca trustpoint *trustpoint-name*

Exemple :

```
ciscoasa(config)# crypto ca trustpoint cisco
```

Remarque
Si vous utilisez HTTP comme méthode de transport, vous devez installer un certificat de sécurité via un point de confiance, ce qui est requis pour HTTPS. Recherchez le certificat spécifique à installer à l'adresse URL suivante :

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

Étape 3 Spécifiez une méthode d'inscription de certificat manuelle par copier-coller.

enroll terminal

Exemple :

```
ciscoasa(ca-trustpoint)# enroll terminal
```

Étape 4 Authentifiez la CA nommée. Le nom de la CA doit correspondre au nom du point de confiance spécifié dans la commande **crypto ca trustpoint**. À l'invite, collez le texte du certificat de sécurité.

crypto ca authenticate trustpoint

Exemple :

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

Étape 5 Spécifiez la fin du texte du certificat de sécurité et confirmez l'acceptation du certificat de sécurité saisi.

quit

Exemple :

```
ciscoasa(ca-trustpoint)# quit
%Do you accept this certificate [yes/no]:
yes
```

Configurer les groupes d'alertes d'environnement et d'instantané

Pour configurer les groupes d'alertes d'environnement et d'instantané, procédez comme suit :

Procédure

Entrez dans le mode de configuration des groupes d'alertes.

alert-group-config {**environment** | **snapshot**}

Exemple :

```
ciscoasa(config)# alert-group-config environment
```

Configurer l'abonnement des groupes d'alertes

Pour abonner un profil de destination à un groupe d'alertes, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Activez le groupe d'alertes Smart Call Home spécifié.

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}

Exemple :

```
ciscoasa(cfg-call-home)# alert-group syslog
```

Utilisez le mot clé **all** pour activer tous les groupes d'alertes. Par défaut, tous les groupes d'alertes sont activés.

Étape 3 Entrez en mode de configuration du profil pour le profil de destination indiqué.

profile *profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

Étape 4 Abonnez-vous à tous les groupes d'alertes disponibles.

subscribe-to-alert-group all

Exemple :

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

Étape 5 Abonnez ce profil de destination au groupe d'alertes de configuration.

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

Exemple :

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
```

Le mot clé **periodic** configure le groupe d'alertes de configuration pour la notification périodique. La période par défaut est quotidienne.

Le mot clé **daily** spécifie l'heure à laquelle l'envoi doit être effectué, au format *hh:mm*, avec une horloge de 24 heures (par exemple, 14:30).

Le mot clé **weekly** spécifie le jour de la semaine et l'heure au format *day hh:mm*, où le jour de la semaine est saisi (par exemple, lundi).

Le mot clé **monthly** spécifie la date numérique, de 1 à 31, et l'heure au format *date hh:mm*.

Configurer les coordonnées du client

Pour configurer les coordonnées du client, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le numéro de téléphone du client. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

phone-number *phone-number-string*

Exemple :

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

Étape 3 Spécifiez l'adresse du client, qui est une chaîne de format libre pouvant comporter jusqu'à 255 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

street-address *street-address*

Exemple :

```
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

Étape 4 Spécifiez le nom du client, qui peut comporter jusqu'à 128 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

contact-name *contact-name*

Exemple :

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

Étape 5 Spécifiez l'ID de client Cisco, qui peut comporter jusqu'à 64 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

customer-id *customer-id-string*

Exemple :

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

Étape 6 Spécifiez l'ID de site du client, qui peut comporter jusqu'à 64 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

site-id *site-id-string*

Exemple :

```
ciscoasa(cfg-call-home)# site-id site1234
```

Étape 7 Spécifiez l'identification du contrat du client, qui peut comporter jusqu'à 128 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

contract-id *contract-id-string*

Exemple :

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

Exemple

L'exemple suivant montre comment configurer les coordonnées :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

Configurer le serveur de messagerie

Nous vous conseillons d'utiliser HTTPS pour le transport des messages, car il est le plus sécurisé. Cependant, vous pouvez configurer une destination de courriel pour Smart Call Home, puis configurer le serveur de messagerie pour qu'il utilise le transport par courriel.

Pour configurer le serveur de messagerie, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le serveur de messagerie SMTP.

mail-server*ip-address* **name priority** [**1-100**] [**all**]

Exemple :

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

Vous pouvez spécifier jusqu'à cinq serveurs de messagerie, en utilisant cinq commandes distinctes. Vous devez configurer au moins un serveur de messagerie pour utiliser le transport par courriel des messages Smart Call Home.

Plus le numéro est bas, plus la priorité du serveur de messagerie est élevée.

L'argument *ip-address* peut être une adresse de serveur de messagerie IPv4 ou IPv6.

Exemple

L'exemple suivant montre comment configurer un serveur de messagerie principal (nommé « smtp.exemple.com ») et un serveur de messagerie secondaire à l'adresse IP 10.10.1.1 :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

Configurer la limitation de débit du trafic

Pour configurer la limitation de débit du trafic, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le nombre de messages que Smart Call Home peut envoyer par minute. La valeur par défaut est de 10 messages par minute.

rate-limit *msg-count*

Exemple :

```
ciscoasa(cfg-call-home)# rate-limit 5
```

Envoyer des communications à Smart Call Home

Pour envoyer des communications Smart Call Home spécifiques, procédez comme suit :

Procédure

Choisissez une des options suivantes :

- Option 1 : envoyer manuellement un message de test à l'aide d'une configuration de profil.

call-home test [*test-message*] **profile** *profile-name*

Exemple :

```
ciscoasa# call-home test [testing123] profile CiscoTAC-1
```

- Option 2 : envoyer un message de groupe d'alertes à un profil de destination, si il est spécifié. Si aucun profil n'est spécifié, envoyez des messages à tous les profils inscrits aux groupes d'alertes d'inventaire, de configuration, d'instantané ou de télémétrie.

  call-home send alert-group inventory { | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

  Exemple :

  ```
  ciscoasa# call-home send alert-group inventory
  ```

- Option 3 : envoyer la sortie de commande à une adresse courriel. La commande de l'interface de ligne de commande spécifiée peut être n'importe quelle commande, y compris les commandes pour tous les modules enregistrés.

  call-home send*cli command* [**email** *email*]

  Exemple :

  ```
  ciscoasa# call-home send cli destination email username@example.com
  ```

  Si vous spécifiez une adresse courriel, la sortie de la commande est envoyée à cette adresse. Si aucune adresse courriel n'est spécifiée, la sortie est envoyée au TAC de Cisco. Le courriel est envoyé au format texte de journal avec le numéro de service, si il est spécifié, dans la ligne d'objet.

  Le numéro de service est requis uniquement si aucune adresse courriel n'est spécifiée ou si une adresse courriel du TAC de Cisco est spécifiée.

Configurer un profil de destination

Pour configurer un profil de destination pour le courriel ou pour HTTP, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Entrez en mode de configuration du profil pour le profil de destination indiqué. Si le profil de destination spécifié n'existe pas, il est créé.

profile *profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# profile newprofile
```

Vous pouvez créer un maximum de 10 profils actifs. Le profil par défaut consiste à renvoyer les renseignements au TAC de Cisco. Si vous souhaitez envoyer des renseignements de connexion à un autre emplacement (par exemple, votre propre serveur), vous pouvez configurer un profil distinct.

Étape 3 Configurez la destination, la taille du message, le format du message et la méthode de transport pour le récepteur de messages Smart Call Home. Le format de message par défaut est XML et la méthode de transport activée par défaut est le courriel.

destination address {**email** *address* | **http** *url*[**reference-identity** *ref-id-name*]} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

Exemple :

```
ciscoasa(cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService reference-identity
ExampleService
ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

L'option **reference-identity** active les vérifications d'identité de référence RFC 6125 sur le certificat de serveur reçu. Celles-ci s'appliquent uniquement aux destinations configurées avec une adresse HTTP. Les vérifications d'ID sont effectuées en fonction d'un objet d'identité de référence précédemment configuré. Consultez Configurer les identités de référence, à la page 910 pour en savoir plus sur l'objet d'identité de référence.

L'e-mail-address est l'adresse courriel du destinataire du message Smart Call Home, qui peut comporter jusqu'à 100 caractères. Par défaut, la taille maximum de l'URL est de 5 Mo.

Utilisez le format de texte court pour envoyer et lire un message sur un appareil mobile et utilisez le format de texte long pour envoyer et lire un message sur un ordinateur.

Si le récepteur du message est le serveur principal Smart Call Home, assurez-vous que la valeur **preferred-msg-format** est XML, car le serveur dorsal n'accepte que les messages au format XML.

Utilisez cette commande pour rétablir la méthode de transport par courriel.

Copier un profil de destination

Pour créer un nouveau profil de destination en copiant un profil existant, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le profil à copier.

profile *profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# profile newprofile
```

Étape 3 Copiez le contenu d'un profil existant vers un nouveau profil.

copy profile *src-profile-name dest-profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

Le profil existant (*src-profile-name*) et le nouveau profil (*dest-profile-name*) peuvent comporter jusqu'à 23 caractères.

Exemple

L'exemple suivant montre comment copier un profil existant :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

Renommer un profil de destination

Pour modifier le nom d'un profil existant, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le profil à renommer.

profile *profilename*

Exemple :

```
ciscoasa(cfg-call-home)# profile newprofile
```

Étape 3 Modifiez le nom d'un profil existant.

rename profile *src-profile-name dest-profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

Le profil existant (*src-profile-name*) et le nouveau profil (*dest-profile-name*) peuvent comporter jusqu'à 23 caractères.

Exemple

L'exemple suivant montre comment renommer un profil existant :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

Supervision des rapports anonymes et de Smart Call Home

Consultez les commandes suivantes pour superviser les services de création de rapports anonymes et les services Smart Call Home.

- **show call-home detail**

  Cette commande affiche la configuration détaillée de Smart Call Home actuelle.

- **show call-home mail-server status**

  Cette commande affiche l'état actuel du serveur de messagerie.

- **show call-home profile** {profile name | **all**}

  Cette commande affiche la configuration des profils Smart Call Home.

- **show call-home registered-module status** [**all**]

  Cette commande affiche l'état du module enregistré.

- **show call-home statistics**

  Cette commande affiche l'état détaillé de Smart Call Home.

- **show call-home**

  Cette commande affiche la configuration de Smart Call Home actuelle.

- **show running-config call-home**

Cette commande affiche la configuration en cours d'exécution de Smart Call Home actuelle.

- **show smart-call-home alert-group**

  Cette commande affiche l'état actuel des groupes d'alertes Smart Call Home.

- **show running-config all**

  Cette commande affiche les détails du profil d'utilisateur des rapports anonymes.

Exemples de Smart Call Home

L'exemple suivant montre comment configurer le service Smart Call Home :

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly Monday
 23:30
```

Historique des rapports anonymes et de Smart Call Home

Tableau 80 : Historique des rapports anonymes et de Smart Call Home

Nom de la caractéristique	Versions de plateforme	Description
Smart Call Home	8.2(2)	Le service Smart Call Home offre des diagnostics proactifs et des alertes en temps réel sur l'ASA, et assure une meilleure disponibilité du réseau et une efficacité opérationnelle accrue. Nous avons introduit ou modifié les commandes suivantes : **active (call home)**, **call-home, call-home send alert-group, call-home test, contact-email-addr**, **customer-id (call home)**, **destination (call home)**, **profile**, **rename profile**, **service call-home, show call-home, show call-home detail**, **show smart-call-home alert-group**, **show call-home profile**, **show call-home statistics**, **show call-home mail-server status**, **show running-config call-home**, **show call-home registered-module status all**, **site-id**, **street-address**, **subscribe-to-alert-group all**, **alert-group-config**, **subscribe-to-alert-group configuration**, **subscribe-to-alert-group diagnostic**, **subscribe-to-alert-group environment**, **subscribe-to-alert-group inventory periodic**, **subscribe-to-alert-group snapshot periodic**, **subscribe-to-alert-group syslog**, **subscribe-to-alert-group telemetry periodic**.
Rapports anonymes	9.0(1)	Vous pouvez contribuer à l'amélioration de la plateforme ASA en activant les rapports anonymes, qui permettent à Cisco de recevoir en toute sécurité un minimum de renseignements sur les erreurs et l'intégrité d'un appareil. Nous avons introduit les commandes suivantes : **call-home reporting anonymous**, **call-home test reporting anonymous**.
Smart Call Home	9.1(2)	La commande **show local-host** a été remplacée par la commande **show local-host | include interface** pour la création de rapports sur les groupes d'alertes de télémétrie.

Nom de la caractéristique	Versions de plateforme	Description
Smart Call Home	9.1(3)	Un message Smart Call Home est envoyé à Cisco pour signaler des événements de grappe importants si vous avez activé la mise en grappe et configuré Smart Call Home pour vous abonner au groupe d'alertes de diagnostic avec un niveau de gravité Critique. Un message de mise en grappe Smart Call Home est envoyé uniquement pour les trois événements suivants : • Lorsqu'une unité rejoint la grappe • Lorsqu'une unité quitte la grappe • Lorsqu'une unité de grappe devient l'unité de contrôle de grappe Chaque message envoyé comprend les renseignements suivants : • Le nombre de membres actifs dans la grappe • La sortie de la commande **show cluster info** et de la commande **show cluster history** sur l'unité de contrôle de grappe
Identités de référence pour les connexions sécurisées au serveur Smart Call Home	9.6(2)	Le traitement du client TLS prend désormais en charge les règles de vérification de l'identité de serveur définies dans la RFC 6125, section 6. La vérification de l'identité sera effectuée lors de la validation PKI pour les connexions TLS au serveur Smart Call Home. Si l'identité présentée ne correspond pas à l'identité de référence configurée, la connexion n'est pas établie. Nous avons ajouté ou modifié les commandes suivantes : **[no] crypto ca reference-identity**, **call home profile destination address http**.



PARTIE IX

Numéro de référence

- Utilisation de l’interface de commande en ligne, à la page 1543
- Adresses, protocoles et ports, à la page 1553



CHAPITRE 52

Utilisation de l'interface de commande en ligne

Ce chapitre décrit comment utiliser l'interface de ligne de commande sur l'ASA.

Remarque L'interface de ligne de commande utilise une syntaxe similaire et d'autres conventions que l'interface de ligne de commande de Cisco IOS, mais le système d'exploitation d'ASA n'est pas une version du logiciel Cisco IOS. Ne supposez pas qu'une commande de l'interface de ligne de commande Cisco IOS fonctionne avec l'ASA ou a la même fonction sur celui-ci.

- Mode pare-feu et mode de contexte de sécurité, à la page 1543
- Modes de commande et invites, à la page 1544
- Formatage de la syntaxe, à la page 1545
- Commandes abrégées, à la page 1546
- Modification de la ligne de commande, à la page 1546
- Exécution de la commande, à la page 1546
- Aide sur les commandes, à la page 1546
- Afficher la configuration d'exécution, à la page 1547
- Filtrer la sortie de la commande show et more, à la page 1547
- Redirection et ajout de la sortie de la commande show, à la page 1548
- Obtention d'un nombre de lignes pour la sortie de la commande show, à la page 1549
- Pagination de la sortie de commande, à la page 1550
- Ajouter des commentaires, à la page 1550
- Fichiers de configuration de texte, à la page 1550
- Ensembles de caractères pris en charge, à la page 1552

Mode pare-feu et mode de contexte de sécurité

L'ASA fonctionne dans une combinaison des modes suivants :

- Mode pare-feu transparent ou pare-feu routé

  Le mode de pare-feu détermine si l'ASA fonctionne en tant que pare-feu de couche 2 ou 3.

- Mode contexte multiple ou contexte simple

Le mode de contexte de sécurité détermine si l'ASA fonctionne en tant que périphérique unique ou sous plusieurs contextes de sécurité, qui agissent comme des périphériques virtuels.

Certaines commandes ne sont disponibles que dans certains modes.

Modes de commande et invites

L'interface de ligne de commande d'ASA comprend des modes de commande. Certaines commandes ne peuvent être saisies que dans certains modes. Par exemple, pour saisir des commandes qui affichent des renseignements sensibles, vous devez saisir un mot de passe et passer en mode privilégié. Ensuite, pour vous assurer que les modifications de configuration ne sont pas saisies accidentellement, vous devez passer en mode de configuration. Toutes les commandes inférieures peuvent être saisies dans les modes supérieurs. Par exemple, vous pouvez saisir une commande EXEC privilégée en mode de configuration globale.



Remarque Les différents types d'invites sont tous des invites par défaut et, lorsqu'ils sont configurés, ils peuvent être différents.

- Lorsque vous êtes dans la configuration système ou en mode de contexte unique, l'invite commence par le nom d'hôte :

  ```
  ciscoasa
  ```

- Lors de l'impression de la chaîne d'invite, la configuration de l'invite est analysée et les valeurs de mot clé configurées sont imprimées dans l'ordre dans lequel vous avez défini la commande d'invite. Les arguments de mot clé peuvent être les suivants et dans n'importe quel ordre : nom d'hôte, domaine, contexte, priorité, état.

  prompt hostname context priority state

- Lorsque vous êtes dans un contexte, l'invite commence par le nom d'hôte suivi du nom de contexte :

  ```
  ciscoasa/context
  ```

L'invite change en fonction du mode d'accès :

- Mode d'exécution de l'utilisateur

  Le mode d'exécution de l'utilisateur vous permet de voir les paramètres ASA minimum. L'invite du mode d'exécution de l'utilisateur s'affiche comme suit lorsque vous accédez à l'ASA pour la première fois :

  ```
  ciscoasa>
  ```

  ```
  ciscoasa/context>
  ```

- mode d'exécution privilégié

  Le mode d'exécution privilégié vous permet de voir tous les paramètres actuels jusqu'à votre niveau de privilège. Toute commande en mode d'exécution de l'utilisateur fonctionnera en mode d'exécution

privilégié. Saisissez la commande **enable** en mode d'exécution de l'utilisateur, qui nécessite un mot de passe, pour démarrer le mode d'exécution privilégié. L'invite comprend le signe de numéro (#) :

```
ciscoasa#

ciscoasa/context#
```

- Mode de configuration globale

  Le mode de configuration globale vous permet de modifier la configuration de l'ASA. Toutes les commandes d'exécution de l'utilisateur, d'exécution privilégiée et de configuration globale sont disponibles dans ce mode. Saisissez la commande **configure terminal** en mode d'exécution privilégié pour démarrer le mode de configuration globale. L'invite change comme suit :

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- Modes de configuration spécifiques aux commandes

  À partir du mode de configuration globale, certaines commandes entrent dans un mode de configuration spécifique à la commande. Toutes les commandes d'exécution de l'utilisateur, d'exécution privilégiée, de configuration globale et de configuration spécifique à la commande sont disponibles dans ce mode. Par exemple, la commande **interface** entre en mode de configuration d'interface. L'invite change comme suit :

  ```
  ciscoasa(config-if)#

  ciscoasa/context(config-if)#
  ```

Formatage de la syntaxe

Les descriptions de la syntaxe des commandes utilisent les conventions répertoriées dans le tableau suivant.

Tableau 81 : Conventions de syntaxe

Convention	Description
gras	Le texte en caractères gras indique les commandes et les mots clés à entrer mot à mot, comme illustré.
italique	Le texte en italique indique les arguments pour lesquels vous devez fournir des valeurs.
[x]	Les éléments indiqués entre crochets sont optionnels (mot clé ou argument).
|	Une barre verticale indique un choix parmi un ensemble facultatif ou obligatoire de mots clés ou d'arguments.
[x | y]	Les mots-clés ou arguments inscrits entre crochets et séparés par une barre verticale indiquent un choix optionnel.

Convention	Description
{x | y}	Les mots-clés ou arguments inscrits entre accolades et séparés par une barre verticale indiquent un choix obligatoire.
[x {y | z}]	Les ensembles de crochets ou d'accolades imbriqués indiquent des choix facultatifs ou obligatoires parmi des éléments facultatifs ou obligatoires. Des accolades et une barre verticale entre crochets indiquent un choix obligatoire dans un élément facultatif.

Commandes abrégées

Vous pouvez abréger la plupart des commandes en utilisant le moins de caractères uniques possible pour une commande. Par exemple, vous pouvez saisir **wr t** pour afficher la configuration au lieu de saisir la commande complète **write terminal**, ou vous pouvez saisir **en** pour démarrer le mode privilégié et **conf t** pour démarrer le mode de configuration. De plus, vous pouvez saisir **0** pour représenter **0.0.0.0**.

Modification de la ligne de commande

L'ASA utilise les mêmes conventions de modification de ligne de commande que le logiciel Cisco IOS. Vous pouvez afficher toutes les commandes saisies précédemment avec la commande **show history** ou individuellement avec la commande de flèche vers le haut ou **^p**. Une fois que vous avez examiné une commande saisie précédemment, vous pouvez avancer dans la liste avec la commande de flèche vers le bas ou **^n**. Lorsque vous atteignez une commande que vous souhaitez réutiliser, vous pouvez la modifier ou appuyer sur la touche **Entrer** (Entrée) pour la lancer. Vous pouvez également supprimer le mot à gauche du curseur avec **^w** ou effacer la ligne avec **^u**.

L'ASA autorise jusqu'à 512 caractères dans une commande; les caractères supplémentaires sont ignorés.

Exécution de la commande

Pour terminer une commande ou un mot clé après avoir saisi une chaîne partielle, appuyez sur la touche **Tab** (Onglet). L'ASA ne termine la commande ou le mot clé que si la chaîne partielle ne correspond qu'à une seule commande ou mot clé. Par exemple, si vous saisissez **s** et appuyez sur la touche **Tab** (Onglet), l'ASA ne termine pas la commande, car il correspond à plusieurs commandes. Cependant, si vous saisissez **dis**, la clé **Tab** (Onglet) complète la commande **disable**.

Aide sur les commandes

Les informations d'aide sont accessibles à partir de la ligne de commande en saisissant les commandes suivantes :

- **help** *command_name*

  Affiche l'aide pour la commande spécifique.

- *command_name* **?**

Affiche une liste des arguments disponibles.

- *string***?** (aucun espace)

  Répertorie les commandes possibles commençant par la chaîne.

- **?** et **+?**

  Répertorie toutes les commandes disponibles. Si vous saisissez **?**, l'ASA affiche uniquement les commandes disponibles pour le mode actuel. Pour afficher toutes les commandes disponibles, y compris celles des modes inférieurs, saisissez **+?**.



Remarque Si vous souhaitez inclure un point d'interrogation (?) dans une chaîne de commande, vous devez appuyer sur **Ctrl-V** avant de taper le point d'interrogation pour ne pas invoquer par inadvertance l'aide de l'interface de ligne de commande.

Afficher la configuration d'exécution

Pour afficher la configuration d'exécution, utilisez l'une des commandes suivantes :

- **show running-config** [**all**] [*command*]

  Si vous spécifiez **all**, tous les paramètres par défaut s'affichent également. Si vous spécifiez une *commande*, la sortie ne comprend que les commandes associées.



Remarque De nombreux mots de passe sont affichés sous la forme *xxx. Pour afficher les mots de passe en texte brut ou sous forme chiffrée, si une phrase secrète principale est activée, utilisez la commande **more**.

- **more system:running-config**

Filtrer la sortie de la commande show et more

Vous pouvez utiliser la barre verticale (|) avec n'importe quelle commande **show** et inclure une option de filtre et une expression de filtrage. Le filtrage est effectué en faisant correspondre chaque ligne de sortie à une expression régulière, comme le logiciel Cisco IOS. En sélectionnant différentes options de filtre, vous pouvez inclure ou exclure toute la sortie qui correspond à l'expression. Vous pouvez également afficher toute la sortie en commençant par la ligne qui correspond à l'expression.

La syntaxe pour l'utilisation des options de filtrage avec la commande **show** est la suivante :

show *command* | {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

ou

more system:running-config| {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

Remarque La commande **more** vous permet d'afficher le contenu de n'importe quel fichier, et non pas seulement la configuration d'exécution; consultez la référence de commande pour en savoir plus.

Dans cette chaîne de commande, la première barre verticale (|) est l'opérateur et doit être incluse dans la commande. Cet opérateur dirige la sortie de la commande **show** vers le filtre. Dans le schéma de syntaxe, les autres barres verticales (|) indiquent d'autres options et ne font pas partie de la commande.

L'option **include** inclut toutes les lignes de sortie qui correspondent à l'expression régulière. L'option **grep** sans **-v** a le même effet. L'option **exclude** exclut toutes les lignes de sortie correspondant à l'expression régulière. L'option **grep** avec **-v** a le même effet. L'option **begin** affiche toutes les lignes de sortie en commençant par la ligne qui correspond à l'expression régulière.

Remplacez *regexp* par n'importe quelle expression régulière de Cisco IOS. L'expression régulière n'est pas entre guillemets ou doubles guillemets, alors soyez prudent avec les espaces de fin, qui seront utilisés dans l'expression régulière.

Lors de la création d'expressions régulières, vous pouvez utiliser n'importe quel chiffre ou lettre que vous souhaitez faire correspondre. En outre, certains caractères du clavier appelés *métadonnée*s ont une signification particulière lorsqu'ils sont utilisés dans des expressions régulières.

Utilisez **Ctrl + V** pour échapper tous les caractères spéciaux de l'interface de ligne de commande, comme un point d'interrogation (?) ou un onglet. Par exemple, tapez **d[Ctrl+V]?g** pour saisir **d?g** dans la configuration.

Redirection et ajout de la sortie de la commande show

Si la sortie à afficher est importante, l'achèvement de la commande peut prendre beaucoup de temps. Par exemple, vous pourriez penser que le système est bloqué si vous essayez d'afficher un million d'entrées de contrôle d'accès ou un très grand tableau ASP.

Au lieu d'afficher la sortie d'une commande **show** à l'écran, vous pouvez la rediriger vers un fichier sur le périphérique ou dans un emplacement distant. Lors de la redirection vers un fichier sur le périphérique, vous pouvez également ajouter la sortie de la commande au fichier.

show *command* | {**append | redirect**} *url*

- **append** *url* ajoute la sortie à un fichier existant. Spécifiez le fichier en utilisant l'une des options suivantes :
  - **disk0:/**[[*path/*]*filename*] ou **flash:/**[[*path/*]*filename*] : **flash** et **disk0** indiquent la mémoire Flash interne. Vous pouvez utiliser l'une ou l'autre de ces options.
  - **disk1:/**[[*path/*]*filename*] : iIndique la mémoire externe.
- **redirect** *url* crée le fichier spécifié ou le remplace si le fichier existe déjà.
  - **disk0:/**[[*path/*]*filename*] ou **flash:/**[[*path/*]*filename*] : **flash** et **disk0** indiquent la mémoire Flash interne. Vous pouvez utiliser l'une ou l'autre de ces options.
  - **disk1:/**[[*path/*]*filename*] : iIndique la mémoire externe.
  - **smb:/**[[*path/*]*filename*] : indique Server Message Block, un système de fichiers local de serveur UNIX.

- **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]] : indique un serveur SCP. Le **type** peut être l'un des mots clés suivants : **ap** (Mode passif ASCII), **an** (Mode normal ASCII), **ip** (Par défaut – Mode passif binaire), **in** (Mode normal binaire).
- **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]—L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur Secure Copy (SCP).
- **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]] : indique un serveur TFTP. ne peut pas contenir d'espaces. L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur TFTP.

Obtention d'un nombre de lignes pour la sortie de la commande show

Au lieu de voir la sortie réelle de la commande **show**, vous pouvez simplement souhaiter voir le nombre de lignes dans la sortie ou le nombre de lignes qui correspondent à une expression régulière. Vous pouvez ensuite comparer facilement le nombre de lignes avec celui des fois précédentes où vous avez saisi la commande. Cela peut constituer une vérification rapide lorsque vous effectuez des modifications de configuration. Vous pouvez soit utiliser le mot clé **count**, soit ajouter **-c** au mot clé grep.

show *command* | **count** [*regular_expression*]

show *command* | **grep -c** [*regular_expression*]

Remplacez *regular_expression* par n'importe quelle expression régulière de Cisco IOS. L'expression régulière n'est pas entre guillemets ou doubles guillemets, alors soyez prudent avec les espaces de fin, qui seront utilisés dans l'expression régulière. L'expression régulière est facultative; si vous n'en incluez pas, le nombre renvoie le nombre total de lignes dans la sortie non filtrée.

Lors de la création d'expressions régulières, vous pouvez utiliser n'importe quel chiffre ou lettre que vous souhaitez faire correspondre. En outre, certains caractères du clavier appelés métadonnées ont une signification particulière lorsqu'ils sont utilisés dans des expressions régulières. Utilisez Ctrl + V pour échapper tous les caractères spéciaux de l'interface de ligne de commande, comme un point d'interrogation (?) ou un onglet. Par exemple, tapez **d[Ctrl+V]?g** pour entrer **d?g** dans la configuration.

Par exemple, pour afficher le nombre total de toutes les lignes dans la sortie **show running-config** :

```
ciscoasa# show running-config | count
Number of lines which match regexp = 271
```

L'exemple suivant montre comment vous pouvez vérifier rapidement le nombre d'interfaces activées. Le premier montre comment utiliser le mot clé **grep** avec une expression régulière pour filtrer uniquement les lignes qui affichent un état opérationnel. L'exemple suivant ajoute l'option **-c** pour afficher simplement le nombre de lignes plutôt que les lignes de sortie.

```
ciscoasa# show interface | grep is up
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
Interface GigabitEthernet0/1 "inside", is up, line protocol is up

ciscoasa# show interface | grep -c is up
```

```
Number of lines which match regexp = 2
```

Pagination de la sortie de commande

Pour les commandes telles que **help** ou **?**, **show**, **show xlate** ou d'autres commandes qui fournissent de longues listes, vous pouvez déterminer si les informations affichent un écran et s'arrêtent ou permettent à la commande de s'exécuter jusqu'à la fin. La commande **pager** vous permet de choisir le nombre de lignes à afficher avant que l'invite More (Plus) ne s'affiche.

Lorsque la pagination est activée, l'invite suivante apparaît :

```
<--- More --->
```

L'invite More (Plus) utilise une syntaxe similaire à la commande UNIX **more** :

- Appuyez sur la barre **d'espace** pour afficher un autre écran.
- Appuyez sur la touche **Enter** (Entrée) pour afficher la ligne suivante.
- Appuyez sur la touche q pour revenir à la ligne de commande.

Ajouter des commentaires

Vous pouvez précéder une ligne de deux-points (:) pour créer un commentaire. Cependant, le commentaire ne s'affiche que dans le tampon de l'historique des commandes et non dans la configuration. Par conséquent, vous pouvez afficher le commentaire avec la commande **show history** ou en appuyant sur une touche de direction pour récupérer une commande précédente, mais comme le commentaire ne se trouve pas dans la configuration, la commande **write terminal** ne l'affiche pas.

Fichiers de configuration de texte

Cette section décrit comment formater un fichier texte de configuration que vous pouvez télécharger sur l'ASA.

Correspondance des commandes avec les lignes dans le fichier texte

Le fichier de configuration texte comprend des lignes correspondant aux commandes décrites dans ce guide.

Dans les exemples, les commandes sont précédées d'une invite d'interface de ligne de commande. L'invite dans l'exemple suivant est « ciscoasa(config)# » :

```
ciscoasa(config)# context a
```

Dans le fichier de configuration texte, vous n'êtes pas invité à saisir des commandes, l'invite est donc omise :

```
context a
```

Commandes de mode de configuration propres aux commandes

Les commandes de mode de configuration spécifiques aux commandes apparaissent en retrait sous la commande principale lorsqu'elles sont saisies dans la ligne de commande. Les lignes de votre fichier texte n'ont pas besoin d'être mises en retrait, tant que les commandes apparaissent directement après la commande principale. Par exemple, le texte suivant, qui n'est pas en retrait, se lit de la même manière que le texte en retrait :

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

Saisies automatiques de texte

Lorsque vous téléchargez une configuration dans l'ASA, il insère certaines lignes automatiquement. Par exemple, l'ASA insère des lignes pour les paramètres par défaut ou pour l'heure à laquelle la configuration a été modifiée. Vous n'avez pas besoin de saisir ces entrées automatiques lorsque vous créez votre fichier texte.

Commande de ligne

Dans la plupart des cas, les commandes peuvent être placées dans n'importe quel ordre dans le fichier. Cependant, certaines lignes, telles que les ACE, sont traitées dans l'ordre dans lequel elles s'affichent, et l'ordre peut affecter la fonction de la liste d'accès. D'autres commandes peuvent également avoir des exigences de commande. Par exemple, vous devez d'abord saisir la commande **nameif** pour une interface, car de nombreuses commandes ultérieures utilisent le nom de l'interface. De plus, les commandes dans un mode de configuration spécifique aux commandes doivent suivre directement la commande principale.

Commandes non incluses dans la configuration du texte

Certaines commandes n'insèrent pas de lignes dans la configuration. Par exemple, une commande d'exécution telle que **show running-config** n'a pas de ligne correspondante dans le fichier texte.

Mots de passe

Les mots de passe de connexion, d'activation et d'utilisateur sont automatiquement chiffrés avant d'être stockés dans la configuration. Par exemple, la forme chiffrée du mot de passe « cisco » pourrait ressembler à jMorNbK0514fadBh. Vous pouvez copier les mots de passe de configuration sur un autre ASA dans sa forme chiffrée, mais vous ne pouvez pas déchiffrer les mots de passe vous-même.

Si vous saisissez un mot de passe non chiffré dans un fichier texte, l'ASA ne le chiffre pas automatiquement lorsque vous copiez la configuration sur l'ASA. L'ASA le chiffre uniquement lorsque vous enregistrez la configuration en cours d'exécution à partir de la ligne de commande à l'aide de la commande **copy running-config startup-config** ou **write memory**.

Plusieurs fichiers de contexte de Security

Pour plusieurs contextes de sécurité, la configuration complète comprend les éléments suivants :

- Les configurations du contexte de sécurité
- La configuration système, qui identifie les paramètres de base de l'ASA, y compris une liste de contextes
- Le contexte d'administration, qui fournit des interfaces réseau pour la configuration système

  La configuration système ne comprend aucune interface ni aucun paramètre réseau pour elle-même. Au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise un contexte désigné comme contexte d'administration.

Chaque contexte est similaire à une configuration en mode de contexte unique. La configuration système diffère de la configuration de contexte en ce que la configuration système comprend des commandes système uniquement (comme une liste de tous les contextes) alors que d'autres commandes typiques sont absentes (comme de nombreux paramètres d'interface).

Ensembles de caractères pris en charge

L'interface de ligne de commande d'ASA prend actuellement en charge uniquement le codage UTF-8. UTF-8 est le schéma de codage particulier pour les symboles Unicode. Il a été conçu pour être compatible avec un sous-ensemble de symboles ASCII. Les caractères ASCII sont représentés dans UTF-8 comme des caractères d'un octet. Tous les autres caractères sont représentés dans UTF-8 sous forme de symboles multioctets.

Les caractères ASCII imprimables (0x20 à 0x7e) sont entièrement pris en charge. Les caractères ASCII imprimables sont les mêmes que ceux de la norme ISO 8859-1. UTF-8 est un super-ensemble d'ISO 8859-1, de sorte que les 256 premiers caractères (0-255) sont identiques à ISO 8859-1. L'interface de ligne de commande d'ASA prend en charge jusqu'à 255 caractères (caractères multioctets) de la norme ISO 8859-1.



CHAPITRE 53

Adresses, protocoles et ports

Ce chapitre fournit une référence rapide des adresses IP, des protocoles et des applications.

- Adresses IPv4 et filtres d'adresse locale, à la page 1553
- Adresses IPv6, à la page 1557
- Protocoles et applications, à la page 1563
- Ports TCP et UDP, à la page 1564
- Ports et protocoles locaux, à la page 1567
- Types ICMP, à la page 1569

Adresses IPv4 et filtres d'adresse locale

Cette section décrit comment utiliser les adresses IPv4 dans l'ASA. Une adresse IPv4 est un nombre de 32 bits écrits en notation décimale à points : quatre champs de 8 bits (octets) convertis de nombres binaires en nombres décimaux, séparés par des points. La première partie d'une adresse IP identifie le réseau sur lequel réside l'hôte, tandis que la seconde partie identifie l'hôte sur le réseau donné. Le champ de numéro de réseau s'appelle le préfixe réseau. Tous les hôtes sur un réseau donné partagent le même préfixe réseau, mais doivent avoir un numéro d'hôte unique. Dans un réseau avec des classes d'adresses IP, la classe de l'adresse détermine la limite entre le préfixe de réseau et le numéro d'hôte.

Classes

Les adresses IP des hôtes sont divisées en trois classes d'adresses différentes : la classe A, la classe B et la classe C. Chaque classe fixe la limite entre le préfixe réseau et le numéro d'hôte à un point différent dans l'adresse de 32 bits. Les adresses de classe D sont réservées à l'IP de multidiffusion.

- Les adresses de classe A (1.xxx.xxx.xxx à 126.xxx.xxx.xxx) utilisent uniquement le premier octet comme préfixe réseau.
- Les adresses de classe B (128.0.xxx.xxx à 191.255.xxx.xxx) utilisent les deux premiers octets comme préfixe réseau.
- Les adresses de classe C (192.0.0.xxx à 223.255.255.xxx) utilisent les trois premiers octets comme préfixe réseau.

Comme les adresses de classe A ont 16 777 214 adresses d'hôtes et les adresses de classe B de 65 534 hôtes, vous pouvez utiliser le filtrage d'adresse locale pour diviser ces énormes réseaux en sous-réseaux plus petits.

Réseaux privés

Si vous avez besoin d'un grand nombre d'adresses sur votre réseau, et qu'elles n'ont pas besoin d'être acheminées sur Internet, vous pouvez utiliser des adresses IP privées que l'autorité d'attribution de numéros par Internet (IANA) recommande (voir RFC 1918). Les plages d'adresses suivantes sont désignées comme des réseaux privés qui ne doivent pas être annoncés :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

Filtres d'adresse locale

Un filtre d'adresse locale vous permet de convertir un seul réseau de classe A, B ou C en plusieurs réseaux. Avec un filtre d'adresse locale, vous pouvez créer un préfixe de réseau étendu qui ajoute des bits du numéro d'hôte au préfixe de réseau. Par exemple, un préfixe de réseau de classe C est toujours composé des trois premiers octets de l'adresse IP. Mais un préfixe de réseau étendu de classe C utilise également une partie du quatrième octet.

Le filtrage d'adresse locale est facile à comprendre si vous utilisez la notation binaire au lieu de la notation décimale à points. Les bits du filtre d'adresse locale ont une correspondance un-à-un avec l'adresse Internet :

- Les bits sont définis sur 1 si le bit correspondant dans l'adresse IP fait partie du préfixe de réseau étendu.
- Les bits sont définis sur 0 si le bit fait partie du numéro d'hôte.

Exemple 1 : si vous avez l'adresse de classe B 129.10.0.0 et que vous souhaitez utiliser le troisième octet dans le préfixe du réseau étendu au lieu du numéro d'hôte, vous devez spécifier un filtre d'adresse locale 11111111.11111111.11111111.00000000. Ce filtre d'adresse locale convertit l'adresse de classe B en équivalent d'une adresse de classe C, où le numéro d'hôte est composé uniquement du dernier octet.

Exemple 2 : si vous souhaitez utiliser une partie du troisième octet pour le préfixe de réseau étendu, vous devez préciser un filtre d'adresse locale comme 11111111.11111111.11111000.00000000, qui utilise seulement 5 bits du troisième octet pour le préfixe de réseau étendu.

Vous pouvez écrire un filtre d'adresse locale sous forme de masque décimal à points ou de masque /*bits* (« barre oblique *bits* »). Dans l'exemple 1, pour un masque décimal à points, vous convertissez chaque octet binaire en un nombre décimal : 255.255.255.0. Pour un masque /*bits*, vous ajoutez le nombre de 1 : /24. Dans l'exemple 2, le nombre décimal est 255.255.248.0 et le /bits est /21.

Vous pouvez également regrouper plusieurs réseaux de classe C dans un réseau plus vaste en utilisant une partie du troisième octet pour le préfixe de réseau étendu. Par exemple, 192.168.0.0/20.

Déterminer le filtre d'adresse locale

Consultez le tableau suivant pour déterminer le filtre d'adresse locale en fonction du nombre d'hôtes souhaité.

Remarque Le premier et le dernier numéro d'un sous-réseau sont réservés, à l'exception de /32, qui identifie un seul hôte.

Tableau 82 : Hôtes, bits et masques décimaux à points

Hôtes	/Masque de bits	Masque décimal à points
16,777,216	/8	Réseau de classe A 255.0.0.0
65,536	/16	Réseau de classe B 255.255.0.0
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	Réseau de classe C 255.255.255.0
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
Ne pas utiliser	/31	255.255.255.254
1	/32	Adresse d'hôte unique 255.255.255.255

Déterminer l'adresse à utiliser avec le filtre d'adresse locale

Les sections suivantes décrivent comment déterminer l'adresse réseau à utiliser avec un filtre d'adresse locale pour un réseau de classe C et de classe B.

Adresse réseau de classe C

Pour un réseau compris entre 2 et 254 hôtes, le quatrième octet tombe sur un multiple du nombre d'adresses d'hôte, en commençant par 0. Par exemple, le tableau suivant montre les sous-réseaux de 8 hôtes (/29) de 192.168.0.x.



Remarque La première et la dernière adresses d'un sous-réseau sont réservées. Dans le premier exemple de sous-réseau, vous ne pouvez pas utiliser 192.168.0.0 ou 192.168.0.7.

Tableau 83 : Adresse réseau de classe C

Sous-réseau avec le masque /29 (255.255.255.248)	Plage d'adresses
192.168.0.0	De 192.168.0.0 à 192.168.0.7
192.168.0.8	De 192.168.0.8 à 192.168.0.15
192.168.0.16	De 192.168.0.16 à 192.168.0.31
—	—
192.168.0.248	De 192.168.0.248 à 192.168.0.255

Adresse réseau de classe B

Pour déterminer l'adresse réseau à utiliser avec le filtre d'adresse locale pour un réseau de 254 à 65 534 hôtes, vous devez déterminer la valeur du troisième octet pour chaque préfixe de réseau étendu possible. Par exemple, vous pouvez créer une adresse de sous-réseau comme 10.1.*x*.0, où les deux premiers octets sont fixes, car ils sont utilisés dans le préfixe de réseau étendu, et le quatrième octet est 0, car tous les bits sont utilisés pour le numéro d'hôte.

Pour déterminer la valeur du troisième octet, procédez comme suit :

1. Calculez le nombre de sous-réseaux que vous pouvez créer à partir du réseau en divisant 65 536 (le nombre total d'adresses en utilisant le troisième et le quatrième octet) par le nombre d'adresses d'hôtes souhaitées.

   Par exemple, 65 536 divisés par 4 096 hôtes équivaut à 16. Par conséquent, il existe 16 sous-réseaux de 4 096 adresses chacun dans un réseau de classe B.

2. Déterminez le multiple de la valeur du troisième octet en divisant 256 (le nombre de valeurs pour le troisième octet) par le nombre de sous-réseaux :

   Dans cet exemple, 256/16 = 16.

   Le troisième octet correspond à un multiple de 16, commençant par 0.

Le tableau suivant présente les 16 sous-réseaux du réseau 10.1.

Remarque La première et la dernière adresses d'un sous-réseau sont réservées. Dans le premier exemple de sous-réseau, vous ne pouvez pas utiliser 10.1.0.0 ou 10.1.15.255.

Tableau 84 : Sous-réseaux du réseau

Sous-réseau avec le masque /20 (255.255.240.0)	Plage d'adresses
10/100	De 10.1.0.0 à 10.1.15.255
10.1.16.0	De 10.1.16.0 à 10.1.31.255
10.1.32.0	De 10.1.32.0 à 10.1.47.255
—	—

Sous-réseau avec le masque /20 (255.255.240.0)	Plage d'adresses
10.1.240.0	De 10.1.240.0 à 10.1.255.255

Adresses IPv6

IPv6 est la prochaine génération de protocole Internet après IPv4. Il fournit un espace d'adressage étendu, un format d'en-tête simplifié, une prise en charge améliorée des extensions et des options, une capacité d'étiquetage des flux, ainsi que des capacités d'authentification et de confidentialité. IPv6 est décrit dans la RFC 2460. L'architecture d'adressage IPv6 est décrite dans la RFC 3513.

Cette section décrit le format et l'architecture de l'adresse IPv6.

Format d'adresses IPv6

Les adresses IPv6 sont représentées par une série de huit champs hexadécimaux de 16 bits séparés par des deux-points (:) au format : x:x:x:x:x:x:x:x. Voici deux exemples d'adresses IPv6 :

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

Remarque Les lettres hexadécimales dans les adresses IPv6 ne sont pas sensibles à la casse.

Vous n'avez pas besoin d'inclure les zéros initiaux dans un champ individuel de l'adresse, mais chaque champ doit contenir au moins un chiffre. Ainsi, l'exemple d'adresse 2001:0DB8:0000:0000:0008:0800:200C:417A peut être raccourci à 2001:0DB8:0:0:8:800:200C:417A en supprimant les zéros initiaux du troisième au cinquième champs à partir de la gauche. Les champs qui contiennent tous des zéros (les troisième et quatrième champs à partir de la gauche) ont été raccourcis à un seul zéro. Les trois zéros initiaux ont été supprimés dans le cinquième champ à partir de la gauche, ce qui a laissé un seul 8 dans ce champ, et le zéro initial a été supprimé dans le sixième champ à partir de la gauche, laissant 800 dans ce champ.

Il est courant que les adresses IPv6 contiennent plusieurs champs hexadécimaux consécutifs de zéros. Vous pouvez utiliser deux signes de deux-points (::) pour compresser des champs consécutifs de zéros au début, au milieu ou à la fin d'une adresse IPv6 (les deux-points représentent les champs hexadécimaux successifs de zéros). Le tableau suivant présente plusieurs exemples de compression d'adresses pour différents types d'adresses IPv6.

Tableau 85 : Exemples de compression d'adresses IPv6

Type d'adresse	Forme standard	Forme compressée
Monodiffusion	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
Multicast (multidiffusion)	FF01:0:0:0:0:0:0:101	FF01::101
Boucle avec retour	0:0:0:0:0:0:0:1	::1

Type d'adresse	Forme standard	Forme compressée
Non défini	0:0:0:0:0:0:0:0	::

Remarque Deux signes de deux-points (::) ne peuvent être utilisés qu'une seule fois dans une adresse IPv6 pour représenter des champs successifs de zéros.

Une autre forme du format IPv6 est souvent utilisée lorsqu'il s'agit d'un environnement contenant des adresses IPv4 et IPv6. Cette alternative a le format x:x:x:x:x:x:y.y.y.y, où x représente les valeurs hexadécimales des six parties de l'adresse IPv6 et y représente les valeurs décimales de la partie IPv4 de 32 bits de l'adresse (qui prend la place des deux autres parties de 16 bits de l'adresse IPv6). Par exemple, l'adresse IPv4 192.168.1.1 pourrait être représentée comme l'adresse IPv6 0:0:0:0:0:0:FFFF:192.168.1.1 ou ::FFFF:192.168.1.1.

Types d'adresses IPv6

Les trois principaux types d'adresses IPv6 sont les suivants :

- **Monodiffusion** : une adresse de monodiffusion est un identifiant pour une seule interface. Un paquet envoyé à une adresse de monodiffusion est livré à l'interface identifiée par cette adresse. Une interface peut avoir plusieurs adresses de monodiffusion.
- **Multidiffusion** : une adresse de multidiffusion est un identifiant pour un ensemble d'interfaces. Un paquet envoyé à une adresse de multidiffusion est transmis à toutes les adresses identifiées par cette adresse.
- **Anycast** : une adresse Anycast est un identifiant pour un ensemble d'interfaces. Contrairement à une adresse de multidiffusion, un paquet envoyé à une adresse Anycast n'est livré qu'à l'interface « la plus proche », comme déterminé par la mesure des distances pour le protocole de routage.

Remarque Il n'y a pas d'adresses de diffusion dans IPv6. Les adresses de multidiffusion fournissent la fonctionnalité de diffusion.

Adresses de monodiffusion

Cette section décrit les adresses de monodiffusion IPv6. Les adresses de monodiffusion identifient une interface sur un nœud de réseau.

Adresse globale

Le format général d'une adresse de monodiffusion globale IPv6 est un préfixe de routage global suivi d'un ID de sous-réseau suivi d'un ID d'interface. Le préfixe de routage global peut être n'importe quel préfixe non réservé par un autre type d'adresse IPv6.

Toutes les adresses de monodiffusion globales, hormis celles commençant par le binaire 000, ont un ID d'interface de 64 bits au format EUI-64 modifié.

Les adresses de monodiffusion globales commençant par le binaire 000 n'ont aucune contrainte quant à la taille ou à la structure de la partie ID d'interface de l'adresse. Un exemple de ce type d'adresse est une adresse IPv6 avec une adresse IPv4 intégrée.

Adresse Site-Local

Les adresses Site-Local sont utilisées pour l'adressage au sein d'un site. Elles peuvent être utilisées pour traiter un site entier sans utiliser de préfixe globalement unique. Les adresses Site-Local ont le préfixe FEC0::/10, suivi d'un ID de sous-réseau de 54 bits, et se terminent par un ID d'interface de 64 bits au format EUI-64 modifié.

Les routeurs Site-Local ne transfèrent pas les paquets qui ont une adresse Site-Local pour une source ou une destination à l'extérieur du site. Par conséquent, les adresses Site-Local peuvent être considérées comme des adresses privées.

Adresse Link-Local

Toutes les interfaces doivent avoir au moins une adresse Link-Local. Vous pouvez configurer plusieurs adresses IPv6 par interface, mais une seule adresse Link-Local.

Une adresse Link-Local est une adresse de monodiffusion IPv6 qui peut être configurée automatiquement sur n'importe quelle interface à l'aide du préfixe de lien local FE80::/10 et de l'identifiant d'interface au format EUI-64 modifié. Les adresses Link-Local sont utilisées dans le protocole de découverte de voisin et dans le processus de configuration automatique sans état. Les nœuds ayant une adresse Link-Local peuvent communiquer; ils n'ont pas besoin d'une adresse locale au site ou d'une adresse unique au niveau mondial pour communiquer.

Les routeurs ne transfèrent pas les paquets qui ont une adresse Link-Local pour un contrôleur source ou de destination. Par conséquent, les adresses Link-Local peuvent être considérées comme des adresses privées.

Adresses IPv6 compatibles avec IPv4

Il existe deux types d'adresses IPv6 qui peuvent contenir des adresses IPv4.

Le premier type est l'adresse IPv6 compatible avec IPv4. Les mécanismes de transition IPv6 comprennent une technique permettant aux hôtes et aux routeurs de tunneler de manière dynamique les paquets IPv6 sur l'infrastructure de routage IPv4. Les nœuds IPv6 qui utilisent cette technique se voient attribuer des adresses de monodiffusion IPv6 spéciales qui transportent une adresse IPv4 globale dans les 32 bits de poids faible. Ce type d'adresse est appelé adresse IPv6 compatible avec IPv4 et a le format ::y.y.y.y, où y.y.y.y est une adresse de monodiffusion IPv4.



Remarque L'adresse IPv4 utilisée dans l'adresse IPv6 compatible avec IPv4 doit être une adresse de monodiffusion IPv4 globalement unique.

Le deuxième type d'adresse IPv6, qui contient une adresse IPv4 intégrée, s'appelle l'adresse IPv6 mappée en IPv4. Ce type d'adresse est utilisé pour représenter les adresses des nœuds IPv4 en tant qu'adresses IPv6. Ce type d'adresse est au format ::FFFF:y.y.y.y, où y.y.y.y est une adresse de monodiffusion IPv4.

Adresse non spécifiée

L'adresse non spécifiée, 0:0:0:0:0:0:0:0, indique l'absence d'adresse IPv6. Par exemple, un nœud nouvellement initialisé sur un réseau IPv6 peut utiliser l'adresse non spécifiée comme adresse source dans ses paquets jusqu'à ce qu'il reçoive son adresse IPv6.

Remarque L'adresse IPv6 non spécifiée ne peut pas être attribuée à une interface. Les adresses IPv6 non spécifiées ne doivent pas être utilisées comme adresses de destination dans les paquets IPv6 ou dans l'en-tête de routage IPv6.

Adresse de la boucle avec retour

L'adresse de boucle avec retour, 0:0:0:0:0:0:0:1, peut être utilisée par un nœud pour s'envoyer un paquet IPv6. L'adresse de boucle avec retour dans IPv6 fonctionne de la même manière que l'adresse de boucle avec retour dans IPv4 (127.0.0.1).

Remarque L'adresse de boucle avec retour IPv6 ne peut pas être attribuée à une interface physique. Un paquet qui a l'adresse de boucle avec retour IPv6 comme adresse source ou de destination doit rester dans le nœud qui a créé le paquet. Les routeurs IPv6 ne transfèrent pas les paquets qui ont l'adresse de boucle avec retour IPv6 comme adresse source ou de destination.

Identifiants de l'interface

Les identifiants d'interface dans les adresses de monodiffusion IPv6 sont utilisés pour identifier les interfaces sur une liaison. Ils doivent être uniques dans un préfixe de sous-réseau. Dans de nombreux cas, l'identifiant d'interface est dérivé de l'adresse de la couche de liaison de l'interface. Le même identifiant d'interface peut être utilisé sur plusieurs interfaces d'un seul nœud, tant que ces interfaces sont associées à des sous-réseaux différents.

Pour toutes les adresses de monodiffusion, à l'exception de celles qui commencent par le binaire 000, l'identifiant d'interface doit comporter 64 bits et être généré au format EUI-64 modifié. Le format EUI-64 modifié est créé à partir de l'adresse MAC de 48 bits en inversant le bit universel/local dans l'adresse et en insérant le numéro hexadécimal FFFE entre les trois octets supérieurs et les trois octets inférieurs de l'adresse MAC.

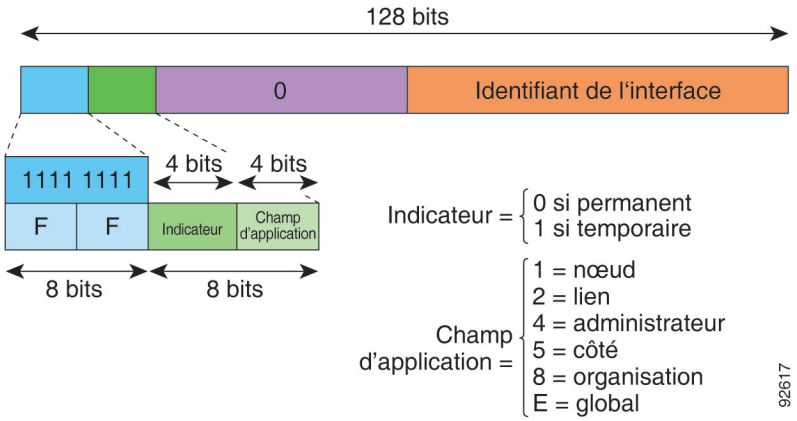
Par exemple, une interface ayant l'adresse MAC 00E0.b601.3B7A aura un ID d'interface de 64 bits 02E0:B6FF:FE01:3B7A.

Multicast Address (Adresse multidiffusion)

Une adresse de multidiffusion IPv6 est un identifiant pour un groupe d'interfaces, généralement sur des nœuds différents. Un paquet envoyé à une adresse de multidiffusion est transmis à toutes les interfaces identifiées par l'adresse de multidiffusion. Une interface peut appartenir à un nombre illimité de groupes de multidiffusion.

Une adresse de multidiffusion IPv6 a un préfixe FF00::/8 (1111 1111). L'octet suivant le préfixe définit le type et la portée de l'adresse de multidiffusion. Une adresse de multidiffusion attribuée de façon permanente (bien connue) a un paramètre d'indicateur égal à 0; une adresse de multidiffusion temporaire (transitoire) a un paramètre d'indicateur égal à 1. Une adresse de multidiffusion qui a la portée d'un nœud, d'une liaison, d'un site ou d'une organisation, ou une portée globale, a un paramètre de portée de 1, 2, 5, 8 ou E, respectivement. Par exemple, une adresse de multidiffusion avec le préfixe FF02::/16 est une adresse de multidiffusion permanente avec une portée de liaison. La figure suivante montre le format d'adresse de multidiffusion IPv6.

Illustration 84 : Format d'adresse de multidiffusion IPv6



Les nœuds IPv6 (hôtes et routeurs) doivent se joindre aux groupes de multidiffusion suivants :

- Les adresses de multidiffusion de tous les nœuds :
  - FF01:: (interface locale)
  - FF02:: (liaison locale)
- L'adresse du nœud sollicité pour chaque adresse de monodiffusion IPv6 et toute adresse Anycast sur le nœud : FF02:0:0:0:0:1:FFXX:XXXX/104, où XX:XXXX correspond aux 24 bits de poids faible de l'adresse de monodiffusion ou de l'adresse Anycast.

Remarque Les adresses de nœud sollicité sont utilisées dans les messages de demande de voisin.

Les routeurs IPv6 doivent se joindre aux groupes de multidiffusion suivants :

- FF01::2 (interface locale)
- FF02::2 (liaison locale)
- FF05::2 (site local)

L'adresse de multidiffusion ne doit pas être utilisée comme adresses source dans les paquets IPv6.

Remarque Il n'y a pas d'adresses de diffusion dans IPv6. Les adresses de multidiffusion IPv6 sont utilisées à la place des adresses de diffusion.

Adresse Anycast

L'adresse Anycast IPv6 est une adresse de monodiffusion attribuée à plusieurs interfaces (appartenant généralement à des nœuds différents). Un paquet qui est acheminé vers une adresse Anycast est acheminé vers l'interface la plus proche ayant cette adresse, la proximité étant déterminée par le protocole de routage en vigueur.

Les adresses Anycast sont attribuées à partir de l'espace d'adressage de monodiffusion. Une adresse Anycast est simplement une adresse de monodiffusion qui a été attribuée à plusieurs interfaces, et les interfaces doivent être configurées pour reconnaître l'adresse comme une adresse Anycast.

Les restrictions suivantes s'appliquent aux adresses Anycast :

- Une adresse Anycast ne peut pas être utilisée comme adresse source pour un paquet IPv6.
- Une adresse Anycast ne peut pas être attribuée à un hôte IPv6; elle ne peut être attribuée qu'à un routeur IPv6.



Remarque Les adresses Anycast ne sont pas prises en charge sur l'ASA.

Adresses requises

Les hôtes IPv6 doivent au moins être configurés avec les adresses suivantes (automatiquement ou manuellement) :

- Une adresse Link-Local pour chaque interface
- L'adresse de boucle avec retour
- Les adresses de multidiffusion de tous les nœuds
- Une adresse de multidiffusion de nœud sollicité pour chaque adresse de monodiffusion ou Anycast

Les routeurs IPv6 doivent au moins être configurés avec les adresses suivantes (automatiquement ou manuellement) :

- Les adresses d'hôte requises
- Les adresses Anycast du routeur de sous-réseau pour toutes les interfaces pour lesquelles il est configuré pour agir en tant que routeur
- Les adresses de multidiffusion de tous les routeurs

Préfixes de l'adresse IPv6

Un préfixe d'adresse IPv6, au format ipv6-prefix/prefix-length, peut être utilisé pour représenter les blocs contigus de bit de l'ensemble de l'espace d'adressage. Le préfixe IPv6 doit être sous la forme documentée dans la RFC 2373, où l'adresse est spécifiée en format hexadécimal en utilisant des valeurs de 16 bits entre les deux-points. La longueur du préfixe est une valeur décimale qui indique le nombre de bits contigus de poids fort de l'adresse qui composent le préfixe (la partie réseau de l'adresse). Par exemple, 2001:0DB8:8086:6502::/32 est un préfixe IPv6 valide.

Le préfixe IPv6 identifie le type d'adresse IPv6. Le tableau suivant affiche les préfixes pour chaque type d'adresse IPv6.

Tableau 86 : Préfixes de type d'adresse IPv6

Type d'adresse	Préfixe binaire	Notation IPv6
Non défini	000...0 (128 bits)	::/128

Type d'adresse	Préfixe binaire	Notation IPv6
Boucle avec retour	000...1 (128 bits)	::1/128
Multicast (multidiffusion)	11111111	FF00::/8
Lien local (monodiffusion)	1111111010	FE80::/10
Site local (monodiffusion)	1111111111	FEC0::/10
Global (monodiffusion)	Toutes les autres adresses.	
Anycast	Tiré de l'espace d'adressage de monodiffusion.	

Protocoles et applications

Le tableau suivant répertorie les valeurs littérales du protocole et les numéros de port; l'un ou l'autre peut être saisi dans les commandes ASA.

Tableau 87 : Valeurs littérales du protocole

Littéral	Valeur	Description
ah	51	En-tête d'authentification pour IPv6, RFC 1826.
eigrp	88	Protocole de routage de passerelle intérieure amélioré.
esp	50	Charge utile de sécurité encapsulée pour IPv6, RFC 1827.
gre	47	Encapsulation générale du routeur.
ICMP	1	Internet Control Message Protocol, RFC 792.
icmp6	58	Internet Control Message Protocol pour IPv6, RFC 2463.
igmp	2	Internet Group Management Protocol, RFC 1112.
igrp	9	Protocole de routage de passerelle intérieure.
ip	0	Protocole Internet.
ipinip	4	Encapsulation IP-en-IP.
IPsec	50	Sécurité IP. La saisie du littéral de protocole ipsec équivaut à la saisie du littéral de protocole esp.
nos	94	Système d'exploitation réseau (NetWare de Novell).
ospf	89	Protocole de routage Open Shortest Path First, RFC 1247.
pcp	108	Protocole de compression de charge utile.
pim	103	Protocol Independent Multicast.

Littéral	Valeur	Description
pptp	47	Protocole Point-to-Point Tunneling. La saisie du littéral de protocole pptp équivaut à la saisie du littéral de protocole gre.
snp	109	Protocole de réseau Sitara.
TCP	6	Protocole de commande de transmission, RFC 793.
UDP	17	Protocole de datagramme d'utilisateur, RFC 768.

Vous pouvez consulter les numéros de protocole en ligne sur le site Web de l'IANA :

http://www.iana.org/assignments/protocol-numbers

Ports TCP et UDP

Le tableau suivant répertorie les valeurs littérales et les numéros de port; l'un ou l'autre peut être saisi dans les commandes ASA. Consultez les avertissements suivants :

- L'ASA utilise le port 1521 pour SQL*Net. Il s'agit du port par défaut utilisé par Oracle pour SQL*Net. Cette valeur n'est toutefois pas conforme aux attributions de ports de l'IANA.
- L'ASA écoute RADIUS sur les ports 1645 et 1646. Si votre serveur RADIUS utilise les ports standard 1812 et 1813, vous pouvez configurer l'ASA pour qu'il écoute ces ports à l'aide des commandes **authentication-port** et **accounting-port**.
- Pour attribuer un port pour l'accès DNS, utilisez la valeur littérale **domain**, et non **dns**. Si vous utilisez **dns**, l'ASA suppose que vous souhaitez utiliser la valeur littérale **dnsix**.

Vous pouvez consulter les numéros de port en ligne sur le site Web de l'IANA :

http://www.iana.org/assignments/port-numbers

Tableau 88 : Valeurs littérales des ports

Littéral	TCP ou UDP?	Valeur	Description
aol	TCP	5190	Amérique en ligne
bgp	TCP	179	Protocole de passerelle frontière, RFC 1163
biff	UDP	512	Utilisé par le système de messagerie pour informer les utilisateurs de la réception d'un nouveau message
bootpc	UDP	68	Client du protocole de démarrage
bootps	UDP	67	Serveur du protocole de démarrage
chargen	TCP	19	Générateur de caractères
cifs	TCP, UDP	3020	Protocole CIFS

Littéral	TCP ou UDP?	Valeur	Description
citrix-ica	TCP	1494	Protocole Citrix Independent Computing Architecture (ICA)
CMD	TCP	514	Similaire à exec, sauf que cmd dispose d'une authentification automatique
ctiqbe	TCP	2748	Encodage rapide de tampon de l'interface de téléphonie de l'ordinateur
daytime	TCP	13	Heure du jour, RFC 867
supprimer	TCP, UDP	9	Supprimer
dnsix	UDP	195	Redirecteur d'audit du module de gestion des sessions DNSIX
domaine	TCP, UDP	53	DNS
echo	TCP, UDP	7	Écho
exec	TCP	512	Exécution du processus à distance
finger	TCP	79	Finger
ftp	TCP	21	Protocole de transfert de fichier (port de contrôle)
données-ftp	TCP	20	Protocole de transfert de fichier (port de données)
gopher	TCP	70	Gopher
h323	TCP	1720	Signalisation d'appel H.323
nom d'hôte	TCP	101	Serveur de noms d'hôte NIC
http	TCP, UDP	80	HTTP Internet
https	TCP	443	HTTP sur SSL
ident	TCP	113	Service d'authentification Ident
imap4	TCP	143	Protocole IMAP (Internet Message Access Protocol), version 4
irc	TCP	194	Protocole de discussion IRC (Internet Relay Chat)
isakmp	UDP	500	protocole ISAKMP (Internet Security Association and Key Management Protocol)
kerberos	TCP, UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell

Littéral	TCP ou UDP?	Valeur	Description
ldap	TCP	389	Protocole Lightweight Directory Access Protocol
ldaps	TCP	636	Protocole Lightweight Directory Access Protocol (SSL)
connexion	TCP	513	Connexion à distance
lotusnotes	TCP	1352	Lotus Notes IBM
lpd	TCP	515	Démon d'impression en ligne – spouleur d'impression
mobile-ip	UDP	434	Agent IP mobile
nameserver	UDP	42	Serveur de noms d'hôte
netbios-dgm	UDP	138	Service de datagrammes NetBIOS
netbios-ns	UDP	137	Service de noms NetBIOS
netbios-ssn	TCP	139	Service de sessions NetBIOS
nfs	TCP, UDP	2049	Système de fichiers réseau – Sun Microsystems
nntp	TCP	119	Protocole de transfert des informations du réseau
ntp	UDP	123	Protocole de synchronisation réseau
pcanywhere-data	TCP	5631	Données pcAnywhere
pcanywhere-status	UDP	5632	État pcAnywhere
pim-auto-rp	TCP, UDP	496	PIM (Protocole Independent Multicast), inondation de chemin inverse, mode dense
pop2	TCP	109	Protocole du bureau de poste – Version 2
pop3	TCP	110	Protocole du bureau de poste – Version 3
pptp	TCP	1723	Protocole Point-to-Point Tunneling
radius	UDP	1645	Service d'usager commuté à authentification distante
radius-acct	UDP	1646	Service d'usager commuté à authentification distante (comptabilité)
protocole RIP	UDP	520	Protocole d'information de routage
rsh	TCP	514	Shell distant
rtsp	TCP	554	Protocole de diffusion en flux continu en temps réel
secureid-udp	UDP	5510	SecureID sur UDP
sip	TCP, UDP	5060	Protocole d'initiation de session (SIP)

Littéral	TCP ou UDP?	Valeur	Description
smtp	TCP	25	Protocole de transport de messagerie simple
snmp	UDP	161	Protocole SNMP (gestion de réseau simple)
snmptrap	UDP	162	Protocole simple de gestion de réseau – Interruption
sqlnet	TCP	1521	Réseau SQL (Structured Query Language)
ssh	TCP	22	Protocole SSH (Secure Shell)
sunrpc	TCP, UDP	111	Appel de procédure à distance Sun
syslog	UDP	514	System Log (journal du système)
tacacs	TCP, UDP	49	Système de contrôle d'accès du contrôleur d'accès du terminal Plus
talk	TCP, UDP	517	Talk
telnet	TCP	23	Telnet RFC 854
tftp	UDP	69	protocole TFTP (Trivial File Transfer Protocol)
de temps	UDP	37	Durée
uucp	TCP	540	Programme de copie UNIX à UNIX
vxlan	UDP	4789	Réseau local extensible virtuel (VXLAN)
who	UDP	513	Qui
Whois	TCP	43	Qui est
www	TCP, UDP	80	Internet
xdmcp	UDP	177	Protocole de contrôle du gestionnaire d'affichage X

Ports et protocoles locaux

Le tableau suivant répertorie les protocoles, les ports TCP et les ports UDP que l'ASA peut ouvrir pour traiter le trafic destiné à l'ASA. À moins que vous activiez les fonctionnalités et les services énumérés dans ce tableau, l'ASA *n'ouvre* aucun protocole local ni port TCP ou UDP. Vous devez configurer une fonctionnalité ou un service pour que l'ASA ouvre le protocole d'écoute ou le port par défaut. Dans de nombreux cas, vous pouvez configurer des ports autres que le port par défaut lorsque vous activez une fonctionnalité ou un service.

Tableau 89 : Protocoles et ports ouverts par les fonctionnalités et services

Fonctionnalité ou service	Protocole	Numéro de port	Commentaires
DHCP (protocole de configuration dynamique des hôtes)	UDP	67,68	—
Contrôle du basculement	105	s.o.	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	S.O.	—
IGMP	2	S. O.	Protocole ouvert uniquement sur l'adresse IP de destination 224.0.0.1
ISAKMP/IKE	UDP	500	Configurable.
IPsec (ESP)	50	S. O.	—
IPsec sur UDP (NAT-T)	UDP	4500	—
IPsec sur TCP (CTCP)	TCP	—	Aucun port par défaut n'est utilisé. Vous devez spécifier le numéro de port lors de la configuration d'IPsec sur TCP.
NTP;	UDP	123	—
OSPF	89	s.o.	Protocole ouvert uniquement sur les adresses IP de destination 224.0.0.5 et 224.0.0.6
Protocole PIM	103	s.o.	Protocole ouvert uniquement sur l'adresse IP de destination 224.0.0.13
RIP	UDP	520	—
Protocole RIPv2	UDP	520	Port ouvert uniquement sur l'adresse IP de destination 224.0.0.9
SNMP	UDP	161	Configurable.
SSH	TCP	22	—
Mise à jour de l'état	8 (non sécurisé) 9 (sécurisé)	S. O.	—
Telnet	TCP	23	—
Équilibrage de la charge VPN	UDP	9023	Configurable.

Fonctionnalité ou service	Protocole	Numéro de port	Commentaires
Mandataire d'authentification de l'utilisateur individuel pour le VPN	UDP	1645, 1646	Port accessible uniquement sur le tunnel VPN.

Types ICMP

Le tableau suivant répertorie les numéros et les noms de type ICMP que vous pouvez saisir dans les commandes ASA.

Tableau 90 : Types ICMP

Numéro ICMP	Nom ICMP
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error

Numéro ICMP	Nom ICMP
32	mobile-redirect

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.