Guide de démarrage Cisco Secure Firewall ASA Virtual, 9.18

Dernière modification : 2025-05-21

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)

© 2022 Cisco Systems, Inc. Tous droits réservés.

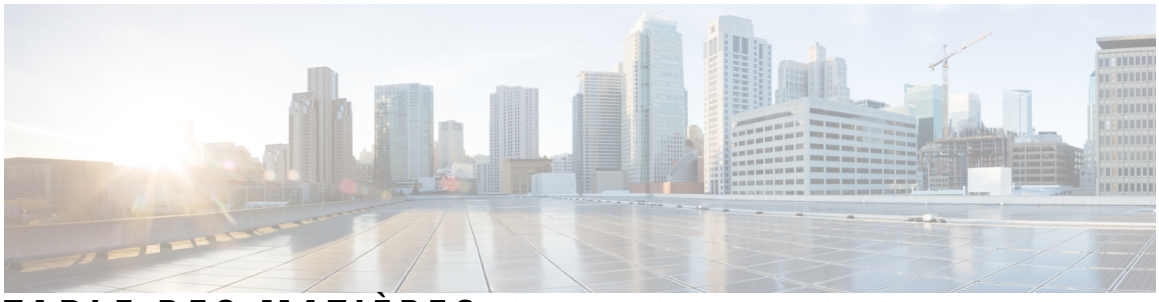


TABLE DES MATIÈRES

CHAPITRE 1 **Introduction à Cisco Secure Firewall ASA Virtual** 1

Prise en charge des hyperviseurs 1

Gestion des licences pour l'ASA virtuel 1

À propos des droits de licence Smart 2

Droits relatifs au cloud privé ASA virtuel (VMware, KVM, Hyper-V) 4

Droits pour le nuage public ASA virtuel (AWS) 4

Droits pour le nuage public ASA virtuel (Azure) 6

Lignes directrices et limites relatives à la licence 7

Lignes directrices et limites pour l'ASA virtuel (tous les droits) 7

Lignes directrices et limites pour le droit de 1 Go 8

Lignes directrices et limites pour le droit de 10 Go 8

Lignes directrices et limites relatives au droit à 20 GO 9

Interfaces et cartes réseau virtuelles d'ASA virtuel 9

Interfaces ASA virtuel 10

vNIC prises en charge 10

ASA virtuel et provisionnement de l'interface SR-IOV 12

Lignes directrices et limites des interfaces SR-IOV 13

CHAPITRE 2 **Déployer l'ASA virtuel à l'aide de VMware** 17

Lignes directrices et limites relatives à la licence 17

Prise en charge des fonctionnalités de VMware pour ASA virtuel 22

Prérequis 23

Décompresser le logiciel ASA virtuel et créer un fichier de configuration de Day 0 (jour 0) 24

Déployer l'ASA virtuel à l'aide du client web VMware vSphere 27

Accéder au client web vSphere et installer le module d'intégration du client 28

Déployer l'ASA virtuel à l'aide du client web VMware vSphere 28

Déployer l'ASA virtuel à l'aide du client autonome VMware vSphere et de la configuration Day0 (Jour0). 33
Déployer l'ASA virtuel à l'aide de l'outil OVF et de la configuration Day0 (Jour0) 34
Accéder à la console ASA virtuel 35
Utiliser la console VMware vSphere 35
Configurer un port de console de série de réseau 36
Mettre à niveau la licence vCPU ou débit 37
Réglage de la performance 38
Amélioration de la performance pour les configurations ESXi 38
Lignes directrices NUMA 39
Files d'attente RX multiples pour le dimensionnement de la réception (RSS). 41
Provisionnement d'interface SR-IOV 43
Lignes directrices et limites relatives à la licence 44
Vérifier le BIOS de l'hôte ESXi 44
Activer SR-IOV sur l'adaptateur physique de l'hôte 45
Créer un commutateur vSphere 46
Mettre à niveau le niveau de compatibilité des machines virtuelles 47
Attribuer la carte NIC SR-IOV à l'ASA virtuel 48

CHAPITRE 3 **Déployer l'ASA virtuel à l'aide de KVM 51**
Lignes directrices et limites relatives à la licence 51
Aperçu 54
Prérequis 54
Préparer le fichier de configuration Day0 (Jour0) 55
Préparer les fichiers XML de pont virtuel 57
Déployer l'ASA virtuel 58
Réglage de la performance 59
Amélioration des performances pour les configurations KVM 59
Activer l'épinglage du processeur (CPU) 60
Lignes directrices NUMA 61
Files d'attente RX multiples pour le dimensionnement de la réception (RSS). 63
Optimisation du réseau privé virtuel (VPN) 66
Provisionnement d'interface SR-IOV 66
Exigences pour le provisionnement de l'interface SR-IOV 66

Modifier le BIOS et le système d'exploitation de l'hôte KVM 66
Affecter des périphériques PCI à l'ASA virtuel 68
Utilisation et rapport d'utilisation du processeur (CPU) 71
Utilisation de vCPU dans ASA virtuel 72
Exemple d'utilisation du processeur 72
Rapport d'utilisation du processeur (CPU) de KVM 72
Graphiques ASA virtuel et KVM 73

CHAPITRE 4 **Déployer l'ASA virtuel sur AWS en nuage 75**
Aperçu 75
Prérequis 78
Lignes directrices et limites relatives à la licence 78
Migration de la configuration et authentification SSH 79
Exemple de topologie de réseau 80
Déploiement ASA virtuel 81
Intégration du service Amazon GuardDuty et Défense contre les menaces virtuelles 84
À propos de l'intégration d'Cisco Secure Firewall ASA virtuel et GuardDuty 84
Procédure de bout en bout 84
Intégration avec le Cisco Secure Firewall device manager à l'aide du groupe d'objets réseau 85
Composants clés de cette intégration 85
Plateformes logicielles prises en charge 87
Lignes directrices et limites pour l'intégration d'Amazon GuardDuty et de Cisco Secure Firewall ASA Virtual 87
Intégrer Amazon GuardDuty avec ASA virtuel 88
Activer le service Amazon GuardDuty sur AWS 88
Télécharger le Cisco Secure Firewall ASA virtuel et le modèle de solution Amazon GuardDuty 89
Configurer vos périphériques gérés pour qu'ils fonctionnent avec Amazon GuardDuty 90
Créer un groupe d'objets réseau 90
Création de comptes d'utilisateur dans ASAv pour l'accès à la fonction Lambda 91
(Facultatif) Chiffrer les mots de passe 91
Préparer les fichiers de ressources d'Amazon GuardDuty pour le déploiement 92
Préparer le fichier d'entrée de la configuration 92
Préparation du fichier d'archive de la fonction Lambda 93
Préparer le fichier de la couche Lambda 94

Charger des fichiers dans le service Amazon Simple Storage 95
Collecter les paramètres d'entrée pour le modèle CloudFormation 96
Déployer la pile 98
S'abonner aux notifications par courriel 98
Valider votre déploiement 99
Mettre à jour la configuration de déploiement de solution existante 100
Réglage de la performance 101
Optimisation du réseau privé virtuel (VPN) 101

CHAPITRE 5 **Déployer la solution d'évolutivité automatique ASA virtuel sur AWS 103**
Solution d'évolutivité automatique pour la Défense contre les menaces virtuelles ASA virtuel sur AWS 103
Aperçu 103
Scénario d'évolutivité automatique 104
Fonctionnement de la solution d'évolutivité automatique 105
Composants de la solution d'évolutivité automatique 105
Prérequis 106
Télécharger les fichiers de déploiement 106
Configuration de l'infrastructure 106
VPC 107
Subnets (Sous-réseaux) 107
Groupes de sécurité 108
Compartiment Amazon S3 108
Certificat de serveur SSL 108
Couche Lambda 108
Clé principale de KMS 109
Environnement Python 3 109
Déployer la solution d'évolutivité automatique 109
Préparation 109
Paramètres d'entrée 109
Mettre à jour les fichiers de configuration ASA 114
Charger des fichiers dans le service de stockage Amazon Simple Storage (S3) 116
Déployer la pile 116
Valider les déploiements 116

Tâches de maintenance 117
Processus d'évolutivité 117
Moniteur d'intégrité 117
Désactiver les crochets de cycle de vie 117
Désactiver le gestionnaire d'évolutivité automatique 117
Cibles de l'équilibreur de charge 118
Instance en veille 118
Mettre fin à une instance 119
Protection de l'instance par l'évolutivité à la baisse 119
Changements de configuration 119
Modifications des ressources AWS 119
Récupérer et analyser les journaux CloudWatch 120
Dépannage et débogage 120

CHAPITRE 6 **Déployer l'ASA virtuel sur Microsoft Azure Cloud** 123
Aperçu 123
Prérequis 125
Lignes directrices et limites relatives à la licence 126
Ressources créées lors du déploiement 129
Routage Azure 130
Configuration du routeur pour les machines virtuelles dans le réseau virtuel 130
Adresses IP 131
DNS 131
Mise en réseau accélérée (AN) 132
Déployer l'ASA virtuel 132
Déployer l'ASA virtuel à partir d'Azure Resource Manager 133
Déployer l'ASA virtuel à partir d'Azure Security Center 134
Déployer l'ASA virtuel pour la haute disponibilité à partir d'Azure Resource Manager 137
Déployer l'ASA virtuel à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources 138
Annexe : Exemple de modèle de ressource Azure 142
Format du fichier du modèle 142
Créer un modèle de ressources 143
Format du fichier des paramètres 149

Créer un fichier de paramètres 152

CHAPITRE 7 **Déployer la solution d'évolutivité automatique ASA virtuel sur Microsoft Azure 155**

Solution d'évolutivité automatique pour ASA virtuel sur Azure 155

Aperçu 155

Scénario d'évolutivité automatique 156

Champ d'application 157

Télécharger le paquet de déploiement 157

Composants de la solution d'évolutivité automatique 157

Prérequis 159

Ressources Azure 159

Préparer le fichier de configuration ASA 159

Créer le paquet d'applications Azure Function 161

Paramètres d'entrée 161

Déployer la solution d'évolutivité automatique 166

Déployer le modèle ARM d'évolutivité automatique 166

Déployer l'application Azure Function 171

Ajustement de la configuration 173

Configurer le rôle IAM dans l'ensemble d'évolutivité des machines virtuelles 175

Mettre à jour les groupes de sécurité 176

Mettre à jour l'application Azure Logic 176

Mettre à niveau l'ASA virtuel 180

Logique d'évolutivité automatique 182

Journalisation et débogage de l'évolutivité automatique 182

Lignes directrices et limites relatives à l'évolutivité automatique 184

Dépannage 184

Créer des fonctions Azure à partir du code source 185

CHAPITRE 8 **Déployer l'ASA virtuel sur Rackspace Cloud 187**

Aperçu 187

Prérequis 188

Réseau Rackspace Cloud 189

Configuration Rackspace Day 0 (jour 0) 190

Déployer l'ASA virtuel 192

Utilisation et rapport d'utilisation du processeur (CPU) 194
Utilisation de vCPU dans ASA virtuel 194
Exemple d'utilisation du processeur 194
Rapport d'utilisation du processeur (CPU) de Rackspace 194
Graphiques ASA virtuel et Rackspace 195

CHAPITRE 9 **Déployer l'ASA virtuel à l'aide d'Hyper-V 197**
Aperçu 197
Lignes directrices et limites relatives à la licence 198
Prérequis 199
Préparer le fichier de configuration Day 0 (jour 0) 200
Déployer l'ASA virtuel avec le fichier de configuration Day 0 (jour 0) à l'aide du gestionnaire Hyper-V 202
Déployer l'ASA virtuel sur Hyper-V à l'aide de la ligne de commande 203
Déployer l'ASA virtuel sur Hyper-V à l'aide du gestionnaire Hyper-V 204
Ajouter un adaptateur réseau à partir du gestionnaire Hyper-V 211
Modifier le nom de l'adaptateur réseau 213
Usurpation d'adresses MAC 214
Configurer l'usurpation d'adresse MAC à l'aide du gestionnaire Hyper-V 214
Configurer l'usurpation d'adresse MAC à l'aide de la ligne de commande 214
Configurer SSH 215
Utilisation et rapport d'utilisation du processeur (CPU) 215
Utilisation de vCPU dans l'ASA virtuel 215
Exemple d'utilisation du processeur 216

CHAPITRE 10 **Déployer l'ASA virtuel sur Oracle Cloud Infrastructure 217**
Aperçu 217
Prérequis 218
Lignes directrices et limites relatives à la licence 218
Exemple de topologie de réseau 220
Déployer l'ASA virtuel 220
Configurer le réseau virtuel en nuage (VCN) 220
Créer le groupe de sécurité réseau 221
Créer la passerelle Internet 221

Créer le sous-réseau 222
Créer l'instance ASA virtuel sur OCI 223
Associer les interfaces 225
Ajouter des règles de routage pour les VNIC associées 225
Accéder à l'instance ASA virtuel sur OCI 226
Se connecter à l'instance ASA virtuel à l'aide de SSH 227
Se connecter à l'instance ASA virtuel à l'aide d'OpenSSH 227
Se connecter à l'instance ASA virtuel à l'aide de PuTTY 228

CHAPITRE 11 **Déployer la solution d'évolutivité automatique ASA virtuel sur OCI 231**
Scénario 231
Prérequis 232
Chiffrer le mot de passe 236
Préparation du fichier de configuration ASA 238
Déployer la solution d'évolutivité automatique 244
Déploiement manuel 244
Déployer la pile Terraform Template-1 244
Déployer les fonctions Oracle 245
Déployer Terraform Template-2 248
Déployer l'évolutivité automatique à l'aide de Cloud Shell 249
Valider le déploiement 249
Mise à niveau 250
Ensembles de systèmes principaux de l'équilibreur de charge 251
Supprimer la configuration d'évolutivité automatique d'OCI 251
Suppression manuelle 251
Supprimer la pile Terraform Template-2 252
Supprimer les fonctions Oracle 253
Supprimer la pile Terraform Template-1 253
Supprimer l'évolutivité automatique à l'aide de Cloud Shell 254

CHAPITRE 12 **Déployer l'ASA virtuel sur Google Cloud Platform 255**
Aperçu 255
Prérequis 257
Lignes directrices et limites relatives à la licence 257

Exemple de topologie de réseau 258
Déployer l'ASA virtuel sur Google Cloud Platform 259
Créer des réseaux vPC 259
Créer les règles de pare-feu 260
Créer l'instance ASA virtuel sur GCP 260
Accéder à l'instance ASA virtuel sur GCP 262
Se connecter à l'instance ASA virtuel à l'aide d'une adresse IP externe 263
Se connecter à l'instance ASA virtuel à l'aide de SSH 263
Se connecter à l'instance ASA virtuel à l'aide de la console de série 264
Se connecter à l'instance ASA virtuel à l'aide de GCloud 264
Utilisation et rapport d'utilisation du processeur (CPU) 265
Utilisation de vCPU dans ASA virtuel 265
Exemple d'utilisation du processeur 265
Rapport d'utilisation du processeur (CPU) de GCP 266
Graphiques ASA virtuel et GCP 266

CHAPITRE 13 **Déployer la solution d'évolutivité automatique de l'ASA virtuel sur GCP 267**
Aperçu 267
À propos de la solution d'évolutivité automatique 267
Scénario d'évolutivité automatique 268
Champ d'application 268
Télécharger le paquet de déploiement 269
Composants de la solution d'évolutivité automatique 269
Prérequis 272
Ressources GCP 272
Préparer le fichier de configuration ASA 273
Créer le paquet de fonction en nuage de GCP 275
Paramètres d'entrée 275
Déployer la solution d'évolutivité automatique 279
Logique d'évolutivité automatique 283
Journalisation et débogage 284
Lignes directrices et limites relatives à la licence 285
Dépannage 286

CHAPITRE 14 **Déployer l'ASA virtuel sur OpenStack** 287

Aperçu 287

Préalables pour l'ASA virtuel et OpenStack 287

Lignes directrices et limites relatives à la licence 288

Configuration système requise 289

Exemple de topologie de réseau 290

Déployer l'ASA virtuel 291

Charger l'image ASA virtuel dans OpenStack 291

Créer l'infrastructure réseau pour OpenStack et ASA virtuel 292

Créer l'instance ASA virtuel sur OpenStack 293

CHAPITRE 15 **Déployer l'ASAv sur Nutanix** 295

Aperçu 295

Lignes directrices et limites relatives à la licence 295

Configuration système requise 298

Comment déployer l'ASAv sur Nutanix 299

Prérequis 299

Charger le fichier QCOW2 dans Nutanix 299

Préparer le fichier de configuration Day0 (Jour0) 300

Déployer l'ASA virtuel 302

Lancer l'ASA virtuel 304

CHAPITRE 16 **Déployer l'ASAv sur Cisco HyperFlex** 305

Lignes directrices et limites relatives à la licence 305

Configuration système requise 308

Déployer l'ASA virtuel 309

Conditions préalables pour l'ASAv et Cisco HyperFlex 309

Télécharger et décompresser le logiciel ASAv 310

Déployer l'ASAv sur Cisco HyperFlex dans vSphere vCenter 311

Accéder à la console ASAv 313

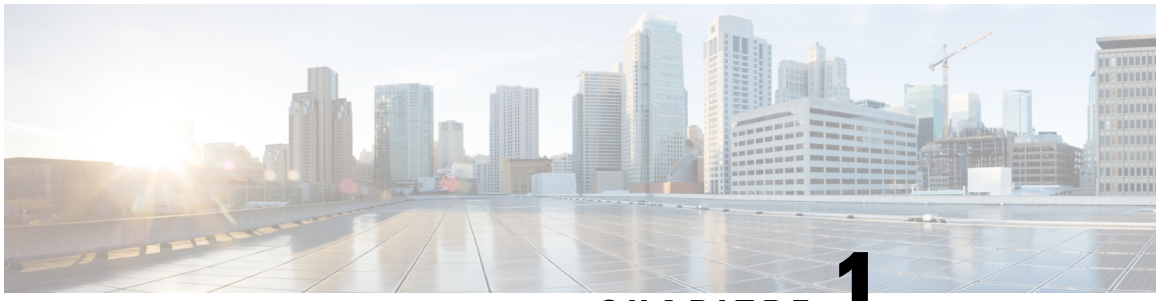
Utiliser la console VMware vSphere 314

Configurer un port de console de série de réseau 315

Mettre à niveau la licence vCPU ou de débit 316

Réglage de la performance 317
Activation des trames étendues 317

CHAPITRE 17 Configurer l’ASA virtuel 319
Démarrer ASDM 319
Effectuer la configuration initiale à l’aide d’ASDM 320
Exécuter l'assistant de démarrage 320
(Facultatif) Autoriser l’accès aux serveurs publics derrière l’ASA virtuel 321
(Facultatif) Exécuter les assistants de réseau privé virtuel (VPN) 321
(Facultatif) Exécuter d’autres assistants dans ASDM 321
Configuration avancée 322



CHAPITRE 1

Introduction à Cisco Secure Firewall ASA Virtual

L'appliance virtuelle de sécurité adaptative (ASA virtuel) offre des fonctionnalités complètes de pare-feu aux environnements virtualisés afin de sécuriser le trafic des centres de données et les environnements multilocataires.

Vous pouvez gérer et surveiller l'ASA virtuel à l'aide d'ASDM ou de l'interface de ligne de commande. D'autres options de gestion peuvent être disponibles.

- Prise en charge des hyperviseurs, à la page 1
- Gestion des licences pour l'ASA virtuel, à la page 1
- Lignes directrices et limites relatives à la licence, à la page 7
- Interfaces et cartes réseau virtuelles d'ASA virtuel, à la page 9
- ASA virtuel et provisionnement de l'interface SR-IOV, à la page 12

Prise en charge des hyperviseurs

Pour la prise en charge des hyperviseurs, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

Gestion des licences pour l'ASA virtuel

L'ASA virtuel utilise les licences logicielles Cisco Smart. Pour des renseignements complets, consultez Gestion des licences logicielles Smart.

Remarque Vous devez installer une licence Smart sur l'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. Une licence Smart est requise pour le fonctionnement normal.

À partir de la version 9.13(1), toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge. Cela vous permet de déployer un ASA virtuel sur une grande variété de profils de ressources VM. Les limites de session pour client AnyConnect et le mandataire TLS sont 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.

Consultez les sections suivantes pour obtenir des renseignements sur les droits de licence d'ASA virtuel et les spécifications de ressources pour les cibles de déploiement privées et publiques prises en charge.

À propos des droits de licence Smart

Toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuelprise en charge. Cela vous permet d'exécuter l'ASA virtuel sur une grande variété de profils de ressources VM. Cela augmente également le nombre d'instances AWS et Azure prises en charge. Lors de la configuration de la machine ASA virtuel, le nombre maximal de vCPU pris en charge est 16 (ASAv100); et la mémoire maximale prise en charge est de 64 Go pour l'ASA virtuel déployé sur toutes les plateformes autres que AWS et OCI. Pour l'ASA virtuel déployé sur AWS et OCI, la mémoire maximum prise en charge est de 128 Go.

Important Il n'est pas possible de modifier l'allocation des ressources (mémoire, CPU, espace disque) d'une instance ASA virtuel une fois qu'elle est déployée. Si vous devez augmenter vos allocations de ressources pour quelque raison que ce soit, par exemple pour modifier vos droits sous licence d'ASAv30/2 Gbit/s à ASAv50/10 Gbit/s, vous devez créer une nouvelle instance avec les ressources nécessaires.

- vCPU : l'ASA virtuel prend en charge de 1 à 16 vCPU.
- Mémoire : l'ASA virtuel prend en charge de 2 Go à 64 Go de RAM pour l'ASA virtuel déployé sur toutes les plateformes à l'exception d'AWS et d'OCI. Pour l'ASA virtuel déployé sur AWS et OCI, la mémoire maximum prise en charge est de 128 Go.
- Stockage sur disque : l'ASA virtuel prend en charge un disque virtuel minimum de 8 Go par défaut. Selon le type de plateforme, la prise en charge du disque virtuel varie entre 8 Go et 10 Go. Gardez cela à l'esprit lorsque vous provisionnez vos ressources de VM.

Important La mémoire minimale requise pour l'ASA virtuel est de 2 Go. Si votre ASA virtuel actuel fonctionne avec moins de 2 Go de mémoire, vous ne pouvez pas effectuer de mise à niveau vers la version 9.13(1) ou une version ultérieure à partir d'une version antérieure sans augmenter la mémoire de votre machine ASA virtuel. Vous pouvez également redéployer une nouvelle machine ASA virtuel avec la dernière version.

La mémoire minimale requise pour le déploiement d'ASA virtuel avec plus d'un vCPU est de 4 Go.

Pour la mise à niveau d'ASA virtuel version 9.14 ou ultérieure vers une dernière version, la machine virtuelle ASA nécessite une mémoire minimale de 4 Go et de 2 vCPU.

Limites de session pour les fonctions sous licence

Les limites de session pour client AnyConnect et le mandataire TLS sont déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée et appliquées par l'intermédiaire d'un limiteur de débit. Le tableau suivant récapitule les limites de session en fonction du niveau d'admissibilité et du limiteur de débit.

Tableau 1 : Limites de session d'ASA virtuel par droit

Autorisation	Paires client AnyConnect Premium	Nombre total de sessions de mandataire TLS	Limiteur de débit
Niveau standard, 100 M	50	500	150 Mbit/sec
Niveau standard, 1 G	250	500	1 Gbit/sec

Autorisation	Paires client AnyConnect Premium	Nombre total de sessions de mandataire TLS	Limiteur de débit
Niveau standard, 2 G	750	1000	2 Gbit/s
Niveau standard, 10 G	10 000	10 000	10 Gbit/s
Niveau standard, 20 G	20 000	20 000	20 Gbit/s

Les limites de session accordées par un droit, comme indiqué dans le tableau précédent, ne peuvent pas dépasser les limites de session de la plateforme. Les limites de session de la plateforme sont basées sur la quantité de mémoire provisionnée pour l'ASA virtuel.

Tableau 2 : Limites de session d'ASA virtuel par exigence de mémoire

Mémoire provisionnée	Paires client AnyConnect Premium	Nombre total de sessions de mandataire TLS
De 2 Go à 7,9 Go	250	500
De 8 Go à 15,9 Go	750	1000
De 16 Go à 31,9 Go	10 000	10 000
De 32 Go à 64 Go	20 000	20 000
De 64 Go à 128 Go	20 000	20 000

Limites de la plateforme

Les connexions de pare-feu, les connexions simultanées et les VLAN sont des limites de plateforme basées sur la mémoire ASA virtuel.

Remarque Nous limitons les connexions de pare-feu à 100 lorsque l'ASA virtuel est dans un état sans licence. Une fois une licence avec n'importe quel droit, les connexions sont acheminées à la limite de la plateforme. La mémoire minimale requise pour l'ASA virtuel est de 2 Go.

Tableau 3 : Limites de la plateforme

Mémoire ASA virtuel	Connexions de pare-feu, simultanées	Réseaux VLAN
De 2 Go à 7,9 Go	100 000	50
De 8 Go à 15,9 Go	500 000	200
De 16 Go à 31,9 Go	2 000 000	1024
De 32 Go à 64 Go	4 000 000	1024

Droits relatifs au cloud privé ASA virtuel (VMware, KVM, Hyper-V)

Étant donné que toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge, vous disposez d'une plus grande flexibilité lorsque vous déployez l'ASA virtuel dans un environnement de cloud privé (VMware, KVM, Hyper-V).

Remarque ASAv50 et ASAv100 ne sont pas pris en charge sur HyperV.

Les limites de session pour client AnyConnect et le mandataire TLS sont déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée et appliquées par l'intermédiaire d'un limiteur de débit. Le tableau suivant récapitule les limites de session en fonction du niveau d'admissibilité de l'ASA virtueldéployé dans un environnement de cloud privé, avec le limiteur de débit appliqué.

Remarque Les limites de session d'ASA virtuel sont basées sur la quantité de mémoire provisionnée pour l'ASA virtuel; voir Tableau 2 : Limites de session d'ASA virtuel par exigence de mémoire, à la page 3.

Tableau 4 : ASA virtuel sur le cloud privé VMware/KVM/HyperV — Limites de fonctionnalités sous licence en fonction des droits

RAM (Go)		Prise en charge des droits*				
Min	**Max**	**Niveau standard, 100 M**	**Niveau standard, 1 G**	**Niveau standard, 2 G**	**Niveau standard, 10 G**	**Niveau standard, 20 G**
2	7,9	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500/20 G
8	15,9	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000/20 G
16	31,9	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K/20 G
32	64	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	20 K/20 K/20 G
*Sessions client AnyConnect/Sessions de mandataire TLS/Limiteur de débit par droit/instance.						

Droits pour le nuage public ASA virtuel (AWS)

Comme toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge, vous pouvez déployer l'ASA virtuel sur de nombreux types d'instances AWS. Les limites de session pour client AnyConnect et le mandataire TLS sont déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée et appliquées par l'intermédiaire d'un limiteur de débit.

Le tableau suivant récapitule les limites de session et le limiteur de débit en fonction du niveau d'admissibilité pour les types d'instance AWS. Consultez « À propos du déploiement d'ASA virtuel sur le nuage AWS » pour obtenir une ventilation des dimensions de la VM AWS (vCPU et mémoire) pour les instances prises en charge.

Tableau 5 : ASA virtuel sur AWS – Limites des fonctionnalités sous licence en fonction des droits

Instance	Prise en charge des droits BYOL*				PAYG**
	Niveau standard, 100 M	Niveau standard, 1 G	Niveau standard, 2 G	Niveau standard, 10 G	
c5.xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000
c5.2xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K
c4.large	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
c4.xlarge	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
c4.2xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	750/1 000
c3.large	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
c3.xlarge	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
c3.2xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	750/1 000
m4.large	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
m4.xlarge	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	10 K/10 K
m4.2xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K

*Sessions client AnyConnect/Sessions de mandataire TLS/Limiteur de débit par droit/instance.

**Sessions client AnyConnect/Sessions de mandataire TLS. Le limiteur de débit n'est pas utilisé en mode PAYG.

Mode Pay-As-You-Go (PAYG)

Le tableau suivant résume les droits de licence Smart pour chaque niveau du mode de facturation à l'heure (PAYG), qui est basé sur la mémoire allouée.

Tableau 6 : ASA virtuel sur AWS – droits de licence Smart pour PAYG

RAM (Go)	Droit pour le mode de facturation à l'heure
< 2 Go	Niveau standard, 100 M (ASAv5)
2 Go à < 8 Go	Niveau standard, 1 G (ASAv10)
8 Go à < 16 Go	Niveau standard, 2 G (ASAv30)
16 Go à < 32 Go	Niveau standard, 10 G (ASAv50)
30 Go et plus	Niveau standard, 20 G (ASAv100)

Droits pour le nuage public ASA virtuel (Azure)

Comme toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge, vous pouvez déployer l'ASA virtuel sur de nombreux types d'instances Azure. Les limites de session pour client AnyConnect et le mandataire TLS sont déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée et appliquées par l'intermédiaire d'un limiteur de débit.

Le tableau suivant récapitule les limites de session et le limiteur de débit en fonction du niveau d'admissibilité pour les types d'instance Azure. Consultez « À propos du déploiement d'ASA virtuel sur le nuage Microsoft Azure » pour obtenir une ventilation des dimensions de la VM Azure (vCPU et mémoire) pour les instances prises en charge.

Remarque Actuellement, le mode Pay-As-You-Go (PAYG) n'est pas pris en charge pour l'ASA virtuel sur Azure.

Tableau 7 : ASA virtuel sur Azure – Limites des fonctionnalités sous licence en fonction des droits

Instance	Prise en charge des droits BYOL*				
	Niveau standard, 100 M	Niveau standard, 1 G	Niveau standard, 2 G	Niveau standard, 10 G	Niveau standard, 20 G
D1, D1_v2DS1, DS1_v2	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500/20 G
D2, D2_v2, DS2, DS2_v2	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500/20 G
D3, D3_v2, DS3, DS3_v2	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000/20 G
D4, D4_v2, DS4, DS4_v2	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K/20 G
D5, D5_v2, DS5, DS5_v2	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/20 K/20 G
D2_v3	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000/20 G
D4_v3	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K/20 G
D8_v3	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K/20 G
F4, F4s	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000/20 G
F8, F8s	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/20 K/20 G
F16, F16s	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/20 K/20 G
*Sessions client AnyConnect/Sessions de mandataire TLS/Limiteur de débit par droit/instance.					

Lignes directrices et limites relatives à la licence

La fonctionnalité de pare-feu ASA virtuel est très similaire aux pare-feu matériel ASA, mais avec les lignes directrices et les limites suivantes.

Lignes directrices et limites pour l'ASA virtuel (tous les droits)

Lignes directrices relatives aux licences Smart

- Le nombre maximum de vCPU pris en charge est de 16. La mémoire maximum prise en charge est de 64 Go pour l'ASA virtuel déployé sur toutes les plateformes à l'exception d'AWS et d'OCI. Pour l'ASA virtuel déployé sur AWS et OCI, la mémoire maximum prise en charge est de 128 Go. Toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuelprise en charge.
- Les limites de session pour les fonctionnalités sous licence et les capacités de plateforme sans licence sont définies en fonction de la quantité de mémoire de VM
- Les limites de session pour client AnyConnect et le mandataire TLS sont déterminées par les droits de plateforme d'ASA virtuel; les limites de session ne sont plus associées à un type de modèle ASA virtuel (ASAv5/10/30/50/100).
- Les limites de session ont une exigence de mémoire minimum; dans les cas où la mémoire de VM est inférieure au minimum d'exigence, les limites de session seront définies pour le nombre maximum pris en charge par la quantité de mémoire.
- Il n'y a aucune modification des droits existants; l'UGS de droit et le nom d'affichage continueront d'inclure le numéro de modèle (ASAv5/10/30/50/100).
- Le droit définit le débit maximum par l'intermédiaire d'un limiteur de débit.
- Il n'y a aucune modification du processus de commande des clients.

Stockage sur disque

L'ASA virtuel prend en charge un disque virtuel maximum de 8 Go par défaut. Vous ne pouvez pas augmenter la taille du disque au-delà de 8 Go. Gardez cela à l'esprit lorsque vous provisionnez vos ressources de VM.

Directives relatives au mode contextuel

Pris en charge en mode contexte unique uniquement Ne prend pas en charge le mode contexte multiple.

Lignes directrices relatives au basculement pour la haute disponibilité

Pour les déploiements de basculement, assurez-vous que l'unité de secours a les mêmes droits de licence; par exemple, les deux unités doivent avoir le droit de 2 Gbit/s.

Important Lors de la création d'une paire à haute accessibilité à l'aide d'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.

Fonctionnalités ASA non prises en charge

L'ASA virtuel ne prend pas en charge les fonctionnalités ASA suivantes :

- Mise en grappe (pour tous les droits, sauf KVM et VMware)
- Mode contexte multiple
- Basculement actif/actif
- EtherChannels
- Licences partagées AnyConnect Premium

Restrictions

- L'ASA virtuel n'est pas compatible avec le pilote d'hôte i40en de 1.9.5 pour la carte réseau x710. Les versions de pilote plus anciennes ou plus récentes fonctionneront. (VMware uniquement)

Lignes directrices et limites pour le droit de 1 Go

Lignes directrices relatives aux performances

- La réservation de bâtis grand format sur plateforme de 1 Go avec 9 interfaces e1000 configurées ou plus peut entraîner le rechargement de l'appareil. Si la **jumbo-frame reservation** (réservation de bâtis grand format) est activée, réduisez le nombre d'interfaces à 8 ou moins. Le nombre exact d'interfaces dépendra de la quantité de mémoire nécessaire pour le fonctionnement des autres fonctionnalités configurées. Il pourrait être inférieur à 8.

Lignes directrices et limites pour le droit de 10 Go

Lignes directrices relatives aux performances

- Prend en charge 10 Gbit/s de trafic agrégé.
- Prend en charge les pratiques suivantes pour améliorer les performances d'ASA virtuel :
  - Nombre de nœuds
  - Plusieurs files d'attente RX
  - Provisionnement SR-IOV
  - Reportez-vous à Réglage de la performance, à la page 38 et à Réglage de la performance, à la page 59 pour en savoir davantage.

- L'épinglage du CPU est recommandé pour atteindre des débits maximum; voir Amélioration de la performance pour les configurations ESXi, à la page 38 et Amélioration des performances pour les configurations KVM, à la page 59.
- La réservation de bâtis grand format avec un ensemble d'interfaces e1000 et i40e-vf peut faire en sorte que les interfaces i40e-vf restent inactives. Si **jumbo-frame reservation** (réservation bâtis grand format) est activé, ne mélangez pas les types d'interface qui utilisent les pilotes e1000 et i40e-vf.

Restrictions

- Le mode transparent n'est pas pris en charge.
- L'ASA virtuel n'est pas compatible avec le pilote d'hôte i40en de 1.9.5 pour la carte réseau x710. Les versions de pilote plus anciennes ou plus récentes fonctionneront. (VMware uniquement)
- Non pris en charge sur Hyper-V.

Lignes directrices et limites relatives au droit à 20 GO

Lignes directrices relatives aux performances

- Prend en charge 20 Gbit/s de trafic agrégé.
- Prend en charge les pratiques suivantes pour améliorer les performances d'ASA virtuel :
  - Nombre de nœuds
  - Plusieurs files d'attente RX
  - Provisionnement SR-IOV
  - Reportez-vous à Réglage de la performance, à la page 38 et à Réglage de la performance, à la page 59 pour en savoir davantage.
- L'épinglage du CPU est recommandé pour atteindre des débits maximum; voir Amélioration de la performance pour les configurations ESXi, à la page 38 et Amélioration des performances pour les configurations KVM, à la page 59.

Restrictions

- L'ASA virtuel n'est pas compatible avec le pilote d'hôte i40en de 1.9.5 pour la carte réseau x710. Les versions de pilote plus anciennes ou plus récentes fonctionneront. (VMware uniquement)
- Le mode transparent n'est pas pris en charge.
- Non pris en charge sur Amazon Web Services (AWS) et Hyper-V.

Interfaces et cartes réseau virtuelles d'ASA virtuel

En tant qu'invité sur une plateforme virtualisée, l'ASA virtuel utilise les interfaces réseau de la plateforme physique sous-jacente. Chaque interface ASA virtuel est mappée à une carte réseau virtuelle (vNIC).

- Interfaces ASA virtuel
- vNIC prises en charge

Interfaces ASA virtuel

L'ASA virtuel comprend les interfaces Gigabit Ethernet suivantes :

- Management 0/0

  Pour AWS et Azure, Management 0/0 peut être une interface « externe » d'acheminement du trafic.

- GigabitEthernet 0/0 jusqu'à 0/8. Notez que le GigabitEthernet 0/8 est utilisé pour la liaison de basculement lorsque vous déployez l'ASA virtuel dans le cadre d'une paire de basculement.

Remarque Pour simplifier la migration de la configuration, dix interfaces GigabitEthernet, comme celles disponibles sur le pilote VMXNET3, portent la mention GigabitEthernet. Cela n'a aucune incidence sur la vitesse d'interface réelle et est uniquement cosmétique.

L'ASA virtuel définit les interfaces GigabitEthernet à l'aide du pilote E1000 comme des liens de 1 Gbit/s. Notez que VMware ne recommande plus d'utiliser le pilote E1000.

- Hyper-V prend en charge jusqu'à huit interfaces. Management 0/0 et GigabitEthernet 0/0 jusqu'à 0/6. Vous pouvez utiliser GigabitEthernet 0/6 comme liaison de basculement.

vNIC prises en charge

L'ASA virtuel prend en charge les vNIC suivantes. Le mélange de vNIC, tels que e1000 et vmxnet3, sur le même ASA virtuel n'est pas pris en charge.

Tableau 8 : vNIC prises en charge

Type de vNIC	Prise en charge des hyperviseurs		ASA virtuelVersion	Notes
	VMware	KVM		
vmxnet3	Oui	Non	Version 9.9(2) ou ultérieure	VMware par défaut Lorsque vous utilisez vmxnet3, vous devez désactiver le Large Receive Offload (LRO, grand déchargement de réception) pour éviter de mauvaises performances TCP. Consultez Désactiver LRO pour VMware et VMXNET3, à la page 11.
e1000	Oui	Oui	Version 9.2(1) ou ultérieure	Non recommandé par VMware.

Type de vNIC	Prise en charge des hyperviseurs		ASA virtuelVersion	Notes
	VMware	KVM		
virtio	Non	Oui	Version 9.3(2.200) ou ultérieure	KVM par défaut
ixgbe-vf	Oui	Oui	Version 9.8(1) ou ultérieure	Par défaut AWS; ESXi et KVM pour la prise en charge de SR-IOV.
i40e-vf	Non	Oui	Version 9.10(1) ou ultérieure	KVM pour la prise en charge de SR-IOV.

Désactiver LRO pour VMware et VMXNET3

Large Receive Offload (LRO) est une technique pour augmenter le débit entrant des connexions réseau à bande passante élevée en réduisant le surdébit du processeur. Elle fonctionne par agrégation de plusieurs paquets entrants d'un seul flux dans un tampon plus grand avant qu'ils ne soient transmis au niveau supérieur de la pile de réseau, réduisant ainsi le nombre de paquets qui doivent être traités. Cependant, la technique LRO peut entraîner des problèmes de performance TCP dans lesquels la livraison des paquets réseau peut ne pas circuler de manière uniforme et pourrait être « en rafale » dans les réseaux congestionnés.

Important VMware active LRO par défaut pour augmenter le débit global. Il est donc nécessaire de désactiver LRO pour les déploiements ASA virtuel sur cette plateforme.

Vous pouvez désactiver LRO directement sur la machine ASA virtuel. Éteignez la machine virtuelle avant d'apporter des modifications à la configuration.

1. Recherchez la machine ASA virtuel dans l'inventaire du client Web vSphere.
    1. Pour trouver une machine virtuelle, sélectionnez un centre de données, un dossier, une grappe, un ensemble de ressources ou un hôte.
    2. Cliquez sur l'onglet **Related Objects** (objets associés), puis sur **Virtual Machines** (machines virtuelles).
2. Faites un clic droit sur la machine virtuelle et sélectionnez **Edit Settings** (modifier les paramètres).
3. Cliquez sur **VM Options** (options de machine virtuelle).
4. Développez **Advanced** (avancé).
5. Sous Configuration Parameters (paramètres de configuration), cliquez sur le bouton **Edit Configuration** (modifier la configuration).
6. Cliquez sur **Add Parameter** (ajouter un paramètre) et saisissez un nom et une valeur pour les paramètres LRO :
    - Net.VmxnetSwLROSL | 0
    - Net.Vmxnet3SwLRO | 0
    - Net.Vmxnet3HwLRO | 0

- Net.Vmxnet2SwLRO | 0
- Net.Vmxnet2HwLRO | 0

Remarque En option, si les paramètres LRO existent, vous pouvez également examiner les valeurs et les modifier au besoin. Si un paramètre est égal à 1, LRO est activé. S'il est égal à 0, LRO est désactivé.

7. Cliquez sur **OK** pour enregistrer vos modifications et quitter la boîte de dialogue **Configuration Parameters** (paramètres de configuration).
8. Cliquez sur **Save** (enregistrer).

Consultez les articles d'assistance de VMware suivants pour plus d'informations :

- VMware KB 1027511
- VMware KB 2055140

ASA virtuel et provisionnement de l'interface SR-IOV

La virtualisation des E/S à racine unique (SR-IOV) permet à plusieurs machines virtuelles exécutant divers systèmes d'exploitation invités de partager un seul adaptateur de réseau PCIe dans un serveur d'hôte. SR-IOV permet à une machine virtuelle de déplacer des données directement vers et à partir de l'adaptateur réseau, en contournant l'hyperviseur pour augmenter le débit du réseau et réduire la charge CPU du serveur. Les processeurs de serveur x86 récents comprennent des améliorations de jetons, comme la technologie Intel VT-d, qui facilitent les transferts directs de mémoire et d'autres opérations requises par SR-IOV.

La spécification SR-IOV définit deux types d'appareils :

- Fonction physique (PF) : essentiellement un NIC statique, un PF est un périphérique PCIe complet qui comprend des fonctionnalités SR-IOV. Les PF sont détectés, gérés et configurés comme des périphériques PCIe normaux. Un seul PF peut assurer la gestion et la configuration d'un ensemble de fonctions virtuelles (VF).
- Fonction virtuelle (VF) : comme pour une vNIC dynamique, un VF est un périphérique PCIe virtuel complet ou allégé qui fournit au moins les ressources nécessaires pour les déplacements de données. Un VF n'est pas géré directement, mais il est dérivé et géré par un PF. Un ou plusieurs VF peuvent être attribués à une machine virtuelle.

Le protocole SR-IOV est défini et géré par le groupe d'intérêts spécial pour l'interconnexion des composants périphériques (PCI SIG), une organisation du secteur qui est agréée pour développer et gérer la norme PCI. Pour en savoir plus sur SR-IOV, consultez Introduction à PCI-SIG SR-IOV : Introduction à la technologie SR-IOV.

Le provisionnement des interfaces SR-IOV sur l'ASA virtuel nécessite une certaine planification, qui commence par le niveau de système d'exploitation, le matériel et le processeur (CPU), les types et les paramètres d'adaptateur appropriés.

Lignes directrices et limites des interfaces SR-IOV

Le matériel spécifique utilisé pour le déploiement ASA virtuel peut varier, selon la taille et les exigences d'utilisation. Gestion des licences pour l'ASA virtuel, à la page 1 explique les scénarios de ressources conformes qui correspondent aux droits de licence pour les différentes plateformes ASA virtuel. En outre, les fonctions virtuelles SR-IOV nécessitent des ressources système spécifiques.

Prise en charge du système d'exploitation de l'hôte et de l'hyperviseur

La prise en charge de SR-IOV et les pilotes VF sont disponibles pour :

- le noyau Linux 2.6.30 ou une version ultérieure

L'ASA virtuel avec les interfaces SR-IOV est actuellement pris en charge sur les hyperviseurs suivants :

- VMware vSphere/ESXi
- QEMU/KVM
- AWS

Prise en charge pour la plateforme matérielle

Remarque Vous devez déployer l'ASA virtuel sur n'importe quel périphérique CPU *de classe de serveur* x86 compatible avec les plateformes de virtualisation prises en charge.

Cette section décrit les lignes directrices matérielles pour les interfaces SR-IOV. Bien qu'il s'agisse de lignes directrices et non d'exigences, l'utilisation de matériel qui ne respecte pas ces lignes directrices peut entraîner des problèmes de fonctionnalité ou de mauvaises performances.

Un serveur prenant en charge SR-IOV et équipé d'un adaptateur PCIe compatible avec SR-IOV est requis. Vous devez être conscient des considérations matérielles suivantes :

- Les capacités des cartes réseau SR-IOV, y compris le nombre de VF disponibles, varient selon les fournisseurs et les périphériques.
- Tous les logements PCIe ne prennent pas en charge SR-IOV.
- Les logements PCIe compatibles avec SR-IOV peuvent avoir des capacités différentes.

Remarque Consultez la documentation de votre fabricant pour connaître la prise en charge de SR-IOV sur votre système.

- Pour les jetons, les cartes-mères et les processeurs compatibles avec VT-d, vous pouvez trouver des renseignements sur cette page de matériel prenant en charge IOMMU compatible avec la virtualisation. VT-d est un paramètre BIOS requis pour les systèmes SR-IOV.
- Pour VMware, vous pouvez effectuer des recherches dans le Guide de compatibilité en ligne pour la prise en charge de SR-IOV.

- Pour KVM, vous pouvez vérifier la compatibilité du processeur. Notez que pour l'ASA virtuel sur KVM, nous prenons uniquement en charge le matériel x86.

Remarque Nous avons testé l'ASA virtuel avec le serveur rack série C Cisco UCS. Notez que le serveur Cisco UCS-B ne prend pas en charge le vNIC ixgbe-vf.

Cartes réseau (NIC) prises en charge pour SR-IOV

- Adaptateur réseau Ethernet Intel X710

Attention L'ASA virtuel n'est pas compatible avec le pilote d'hôte i40en de 1.9.5 pour la carte réseau x710. Les versions de pilote plus anciennes ou plus récentes fonctionneront. (VMware uniquement)

- Adaptateur pour serveur Ethernet Intel X520, DA2

CPU

- CPU multicœur x86_64

  Pont Intel Sandy ou version ultérieure (recommandé).

Remarque Nous avons testé l'ASA virtuel sur le processeur Broadwell d'Intel (E5-2699-v4) à 2,3 GHz.

- Cœurs
  - Au moins 8 cœurs physiques par socket de CPU
  - Les 8 cœurs doivent se trouver sur un seul connecteur.

Remarque L'épinglage de CPU est recommandé pour atteindre le débit maximal sur ASAv50 et ASAv100; consultez Amélioration de la performance pour les configurations ESXi, à la page 38 et Amélioration des performances pour les configurations KVM, à la page 59.

Paramètres BIOS

SR-IOV nécessite une prise en charge dans le BIOS ainsi que dans l'instance de système d'exploitation ou l'hyperviseur qui s'exécute sur le matériel. Vérifiez le BIOS de votre système pour identifier les paramètres suivants :

- SR-IOV est activé

- VT-x (Technologie de virtualisation) est activée
- VT-d est activée
- (Facultatif) Hyperthreading est désactivé

Nous vous recommandons de vérifier le processus avec la documentation du fournisseur, car différents systèmes ont des méthodes différentes pour accéder aux paramètres BIOS et les modifier.

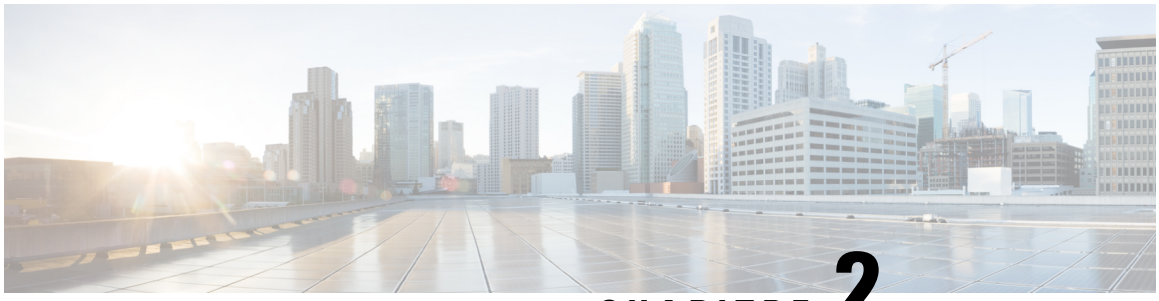
Restrictions

Gardez à l'esprit des limites suivantes lors de l'utilisation des interfaces ixgbe-vf :

- La machine virtuelle invitée n'est pas autorisée à définir le VF en mode promiscuité. Pour cette raison, le mode transparent n'est pas pris en charge lors de l'utilisation de ixgbe-vf.
- La machine virtuelle invitée n'est pas autorisée à définir l'adresse MAC sur le VF. C'est pourquoi l'adresse MAC n'est pas transférée pendant la haute accessibilité, comme cela se fait sur d'autres plateformes ASA et avec d'autres types d'interfaces. Le basculement à haute accessibilité fonctionne par le transfert de l'adresse IP de l'active à la veille.

Remarque Cette limite s'applique également aux interfaces i40e-vf.

- Le serveur Cisco UCS-B ne prend pas en charge la vNIC ixgbe-vf.
- Dans une configuration de basculement, en cas de défaillance d'un ASA virtuel (unité principale) jumelé, l'unité en veille ASA virtuel prend le rôle d'unité principale et l'adresse IP de son interface est mise à jour avec une nouvelle adresse MAC de l'unité en veille ASA virtuel. Ensuite, l'ASA virtuel envoie une mise à jour Gratuitous ARP (Address Resolution Protocol) pour annoncer le changement d'adresse MAC de l'adresse IP de l'interface aux autres périphériques du même réseau. Cependant, en raison d'une incompatibilité avec ces types d'interfaces, la mise à jour Gratuitous ARP n'est pas envoyée à l'adresse IP globale qui est définie dans les instructions NAT ou PAT pour traduire l'adresse IP de l'interface en adresses IP globales.



CHAPITRE 2

Déployer l'ASA virtuel à l'aide de VMware

Vous pouvez déployer l'ASA virtuel sur n'importe quel périphérique CPU de *classe de serveur* x86 compatible avec VMware ESXi.

Important La mémoire minimale requise pour l'ASA virtuel est de 2 Go. Si votre ASA virtuel actuel fonctionne avec moins de 2 Go de mémoire, vous ne pouvez pas effectuer de mise à niveau vers la version 9.13(1)+ à partir d'une version antérieure sans augmenter la mémoire de votre machine ASA virtuel. Vous pouvez également redéployer une nouvelle machine ASA virtuel avec la dernière version.

- Lignes directrices et limites relatives à la licence, à la page 17
- Prise en charge des fonctionnalités de VMware pour ASA virtuel, à la page 22
- Prérequis, à la page 23
- Décompresser le logiciel ASA virtuel et créer un fichier de configuration de Day 0 (jour 0), à la page 24
- Déployer l'ASA virtuel à l'aide du client web VMware vSphere, à la page 27
- Déployer l'ASA virtuel à l'aide du client autonome VMware vSphere et de la configuration Day0 (Jour0)., à la page 33
- Déployer l'ASA virtuel à l'aide de l'outil OVF et de la configuration Day0 (Jour0), à la page 34
- Accéder à la console ASA virtuel, à la page 35
- Mettre à niveau la licence vCPU ou débit, à la page 37
- Réglage de la performance, à la page 38

Lignes directrices et limites relatives à la licence

Vous pouvez créer et déployer plusieurs instances d'ASA virtuel sur un serveur ESXi. Le matériel spécifique utilisé pour les déploiements d'ASA virtuel peut varier en fonction du nombre d'instances déployées et des exigences d'utilisation. Chaque appliance virtuelle que vous créez nécessite une allocation minimale de ressources (mémoire, nombre de CPU et espace disque) sur la machine hôte.

Important L'ASA virtuel est déployé avec une taille de stockage sur disque de 8 Go. Il est impossible de modifier l'allocation des ressources de l'espace disque.

Passez en revue les lignes directrices et les limites suivantes avant de déployer l'ASA virtuel.

ASA virtuel sur les exigences de système VMware ESXi

Assurez-vous de vous conformer aux caractéristiques ci-dessous pour assurer des performances optimales. Les conditions requises par l'ASA virtuelASA virtuel sont les suivantes :

- Le CPU de l'hôte doit être un processeur Intel ou AMD de *classe de serveur* x86 avec extension de virtualisation.

  Par exemple, les laboratoires de tests de performance d'ASA virtuel utilisent au minimum les éléments suivants : Cisco Unified Computing System (Cisco UCS®), serveur série C M4 avec les processeurs Intel Xeon® E5-2690v4 fonctionnant à 2,6 GHz.

- L'ASA virtuel prend en charge ESXi version 6.0, 6.5, 6.7, 7.0, 7.0 mise à niveau 1, 7.0 mise à niveau 2, 7.0 mise à niveau 3.

vNIC recommandées

Les vNIC suivantes sont recommandées pour des performances optimales.

- i40e en mode Transmission directe PCI : dédié à la carte réseau physique du serveur à la machine virtuelle et transfère les données de paquets entre la carte réseau et la machine virtuelle par DMA (accès direct à la mémoire). Aucun cycle de CPU n'est nécessaire pour le déplacement des paquets.

- i40evf/ixgbe-vf : en fait, la même chose que ci-dessus (paquets DMA entre la carte réseau et la VM), mais permet de partager la carte réseau sur plusieurs VM. SR-IOV est généralement préféré, car il offre une plus grande souplesse de déploiement. Voir la section Lignes directrices et limites relatives à la licence, à la page 44.

- vmxnet3 : il s'agit d'un pilote de réseau para-virtualisé qui prend en charge le fonctionnement à 10 Gbit/s, mais nécessite également des cycles du CPU. Il s'agit de la valeur par défaut de VMware.

  Lorsque vous utilisez vmxnet3, vous devez désactiver le Large Receive Offload (LRO, déchargement important à la réception) pour éviter de mauvaises performances TCP.

Optimisation des performances

Pour obtenir les meilleures performances avec ASA virtuel, vous pouvez apporter des ajustements à la machine virtuelle et à l'hôte. Consultez Réglage de la performance, à la page 38 pour de plus amples renseignements.

- **NUMA** : vous pouvez améliorer les performances d'ASA virtuel en isolant les ressources du CPU de la machine virtuelle invitée en un seul nœud d'accès à la mémoire non uniforme (NUMA). Consultez Lignes directrices NUMA, à la page 39 pour de plus amples renseignements.

- **Receive Side Scaling** (Dimensionnement côté réception) : l'ASA virtuel prend en charge Receive Côté Scaling (RSS), qui est une technologie utilisée par les adaptateurs réseau pour distribuer le trafic de réception réseau entre plusieurs cœurs de processeur. Pris en charge à partir de la version 9.13(1). Consultez Files d'attente RX multiples pour le dimensionnement de la réception (RSS)., à la page 41 pour de plus amples renseignements.

- **VPN Optimization** (Optimisation du VPN) : consultez Optimisation du réseau privé virtuel (VPN), à la page 66 pour obtenir des considérations supplémentaires afin d'optimiser les performances du VPN avec l'ASA virtuel.

Mise en grappes

À partir de la version 9.17, la mise en grappe est prise en charge sur les instances d'ASA virtuel déployées sur VMware. Consultez la section Grappe ASA pour l'ASAv pour de plus amples renseignements.

Lignes directrices relatives aux fichiers OVF

La sélection du fichier asav-vi.ovf ou asav-esxi.ovf repose sur la cible de déploiement :

- asav-vi : pour le déploiement sur vCenter
- asav-esxi : pour le déploiement sur ESXi (sans vCenter)
- Le déploiement OVF d'ASA virtuel ne prend pas en charge la localisation (installation des composants en mode non anglais). Assurez-vous que VMware vCenter et les serveurs LDAP de votre environnement sont installés dans un mode compatible avec ASCII.
- Vous devez régler votre clavier à l'anglais des États-Unis avant d'installer l'ASA virtuel et pour utiliser la console de VM.
- Lorsque l'ASA virtuel est déployé, deux images ISO différentes sont montés sur l'hyperviseur ESXi :
  - Le premier disque monté comporte les variables d'environnement OVF générées par vSphere.
  - Le deuxième lecteur monté est day0.so.

Attention Vous pouvez démonter les deux disques après le démarrage de la machine ASA virtuel. Cependant, le lecteur 1 (avec les variables d'environnement OVF) sera toujours monté chaque fois que l'ASA virtuel est mis hors tension ou sous tension, même si la case **Connect at Power On** (Connecter lors de la mise sous tension) n'est pas cochée.

Lignes directrices relatives à l'exportation du modèle OVF

L'option Exporter le modèle OVF dans vSphere vous aide à exporter un ensemble d'instances ASA virtuel existant en tant que modèle OVF. Vous pouvez utiliser un modèle OVF exporté pour déployer l'instance ASA virtuel dans le même environnement ou un environnement différent. Avant de déployer l'instance ASA virtuel à l'aide d'un modèle OVF exporté sur vSphere, vous devez modifier les détails de configuration dans le fichier OVF pour éviter l'échec du déploiement.

Pour modifier le fichier OVF exporté d'ASA virtuel.

1. Connectez-vous à la machine locale où vous avez exporté le modèle OVF.
2. Parcourez le menu et ouvrez le fichier OVF dans un éditeur de texte.
3. Assurez-vous que la balise `<vmw:ExtraConfig vmw:key="monitor_control.pseudo_perfctr" vmw:value="TRUE"></vmw:ExtraConfig>` est présente.
4. Supprimez la balise `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>`.

   Ou

   Remplacez la balise `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>` avec `<rasd:ResourceSubType>vmware.cdrom.remotepassthrough</rasd:ResourceSubType>`.

Consultez le lien Le déploiement d'un fichier OVF échoue sur vCenter Server 5.1/5.5 lorsque les outils VMware sont installés (2034422) publié par VMware pour de plus amples renseignements.

5. Saisissez les valeurs de propriété de `UserPrivilege`, `OvfDeployment` et `ControllerType`.

   Par exemple :

```
- <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
ovf:key="OvfDeployment">
+ <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
ovf:key="OvfDeployment" ovf:value="ovf">

- <Property ovf:type="string" ovf:key="ControllerType">
+ <Property ovf:type="string" ovf:key="ControllerType" ovf:value="ASAv">

- <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege">
+ <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege" ovf:value="15">
```

6. Enregistrez le fichier OVF.
7. Déployez l'ASA virtuel à l'aide du modèle OVF Consultez Déployer l'ASA virtuel à l'aide du client web VMware vSphere.

Lignes directrices relatives au basculement pour la haute disponibilité

Pour les déploiements de basculement, assurez-vous que l'unité de secours a les mêmes droits de licence; par exemple, les deux unités doivent avoir le droit de 2 Gbit/s.

Important Lors de la création d'une paire à haute accessibilité à l'aide d'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.

Pour le groupe de ports ESX utilisé pour l'interface interne d'ASA virtuel ou la liaison de basculement haute disponibilité d'ASA virtuel, configurez l'ordre de basculement du groupe de ports ESX avec deux cartes réseau virtuelles : l'une comme liaison ascendante active et l'autre comme liaison ascendante de secours. Ceci est nécessaire pour que les deux VM s'envoient des messages Ping ou que le lien de haute disponibilité d'ASA virtuel soit activé.

Lignes directrices vMotion

- VMware exige que vous utilisiez le stockage partagé uniquement si vous prévoyez utiliser vMotion. Pendant le déploiement d'ASA virtuel, si vous avez une grappe d'hôtes, vous pouvez provisionner le stockage localement (sur un hôte précis) ou sur un hôte partagé. Cependant, si vous essayez d'utiliser l'ASA virtuel vMotion vers un autre hôte, l'utilisation du stockage local produira une erreur.

Allocation de mémoire et de vCPU pour le débit et les licences

- La mémoire allouée à l'ASA virtuel est d'une taille spécifique pour le niveau de débit. Ne modifiez pas les paramètres de mémoire ni les paramètres matériels de vCPU dans la boîte de dialogue Edit Settings (Modifier les paramètres), sauf si vous demandez une licence pour un autre niveau de débit. Le provisionnement insuffisant peut affecter les performances.

Remarque Si vous devez modifier la mémoire ou les paramètres matériels vCPU, utilisez uniquement les valeurs documentées dans Gestion des licences pour l'ASA virtuel, à la page 1. N'utilisez pas les valeurs minimales, par défaut et maximales de configuration de mémoire recommandées par VMware.

Réservation de CPU

- Par défaut, la réservation de CPU pour l'ASA virtuel est de 1 000 MHz. Vous pouvez modifier la quantité de ressources de CPU allouées à l'ASA virtuel en utilisant les paramètres de partages, de réservations et de limites (Edit Settings > Resources > CPU (Modifier les paramètres > Ressources > CPU)). L'abaissement du paramètre de réservation de CPU de 1 000 MHz peut être effectué si l'ASA virtuel peut réaliser l'objectif requis tout en étant sous la charge de trafic requise avec le paramètre inférieur. La quantité de CPU utilisée par un ASA virtuel dépend de la plateforme matérielle sur laquelle il s'exécute, ainsi que du type et de la quantité de travail qu'il effectue.

  Vous pouvez afficher le point de vue de l'hôte sur l'utilisation du CPU pour toutes vos machines virtuelles à partir du tableau d'utilisation du CPU (MHz), situé dans la vue Home (Accueil) de l'onglet Virtual Machine Performance (Performances de la machine virtuelle). Une fois que vous avez établi un test de référence pour l'utilisation du CPU lorsque l'ASA virtuel traite le volume de trafic typique, vous pouvez utiliser ces renseignements comme entrée pour ajuster la réservation du CPU.

  Consultez le lien Conseil d'amélioration des performances du CPU publié par VMware pour en savoir plus.

- Vous pouvez utiliser les commandes **show vm** et **show cpu** d'ASA virtuel ou l'onglet **Home (Accueil)** > **Device Dashboard (Tableau de bord des appareils)** > **Device Information (Renseignements sur l'appareil)** > **Virtual Resources (Ressources virtuelles)** d'ADSM ou le volet **Monitoring (Supervision)** > **Properties (Propriétés)** > **System Resources Graphs (Graphiques des ressources du système)** > **CPU (Processeur)** pour afficher l'allocation des ressources et toutes les ressources qui sont surprovisionnées ou sous-provisionnées.

- À partir de la version 9.16.x d'ASA virtuel, lorsque vous rétrogradez d'ASAv100, dont la configuration de l'appareil est de 16 vCPU et de 32 Go de RAM, à ASAv10, vous devez configurer l'appareil avec 1 vCPU et 4 Go de RAM.

Lignes directrices relatives au mode transparent sur le matériel UCS de série B

Des intermittences MAC ont été observées dans certaines configurations d'ASA virtuel fonctionnant en mode transparent sur le matériel Cisco UCS de série B. Lorsque des adresses MAC apparaissent à partir de différents emplacements, vous obtiendrez des paquets abandonnés.

Les lignes directrices suivantes aident à éviter les intermittences MAC lorsque vous déployez l'ASA virtuel en mode transparent dans les environnements VMware :

- Regroupement NIC VMware : si vous déployez l'ASA virtuel en mode transparent sur le matériel UCS de série B, les groupes de ports utilisés pour les interfaces interne et externe ne doivent avoir qu'un seul lien ascendant actif, qui doit être le même. Vous configurez le regroupement de NIC VMware dans vCenter.

  Consultez la documentation de VMware pour obtenir des renseignements complets sur la configuration du regroupement NIC.

- Inspection ARP : activez l'inspection ARP sur l'ASA virtuel et configurez de manière statique les entrées MAC et ARP sur l'interface sur laquelle vous souhaitez les recevoir. Consultez le Guide de configuration des opérations générales de la série Cisco Secure Firewall ASA pour en savoir plus sur l'inspection ARP et sur la façon de l'activer.

Directives et limites additionnelles

- L'ASA virtuel démarre sans les deux disques IDE de CD/DVD si vous exécutez ESXi 6.7, vCenter 6.7, ASA Virtual 9.12 et versions ultérieures.
- Le client Web vSphere n'est pas pris en charge pour le déploiement OVF d'ASA virtuel; utilisez plutôt le client vSphere.

Prise en charge des fonctionnalités de VMware pour ASA virtuel

Le tableau suivant énumère la prise en charge des fonctionnalités de VMware pour l'ASA virtuel.

Tableau 9 : Prise en charge des fonctionnalités de VMware pour ASA virtuel

Fonctionnalités	Description	Prise en charge (Oui/Non)	Commentaire
Clonage à froid	La machine virtuelle est hors tension pendant le clonage.	Oui	–
DRS	Utilisé pour la planification dynamique des ressources et la gestion de l'alimentation distribuée.	Oui	Non admissible.
Ajout à chaud	La machine virtuelle est en cours d'exécution pendant un ajout.	Non	–
Clonage à chaud	La machine virtuelle est en cours d'exécution pendant le clonage.	Non	–
Suppression à chaud	La machine virtuelle est en cours d'exécution pendant la suppression.	Non	–
Snapshot	La machine virtuelle se bloque pendant quelques secondes.	Oui	À utiliser avec prudence. Vous pourriez perdre du trafic. Un basculement peut se produire.
Suspendre et reprendre	La machine virtuelle est suspendue, puis reprend.	Oui	–

Fonctionnalités	Description	Prise en charge (Oui/Non)	Commentaire
vCloud Director	Autorise le déploiement automatique des machines virtuelles.	Non	–
Migration de machine virtuelle	La machine virtuelle est hors tension pendant la migration.	Oui	–
vMotion	Utilisé pour la migration en direct des machines virtuelles.	Oui	Utiliser le stockage partagé. Consultez Lignes directrices vMotion, à la page 20.
VMware FT	Utilisé pour la haute disponibilité sur les machines virtuelles.	Non	Utiliser le basculement ASA virtuel pour les défaillances de machine ASA virtuel.
VMware haute disponibilité	Utilisé pour ESXi et les défaillances de serveur.	Oui	Utiliser le basculement ASA virtuel pour les défaillances de machine ASA virtuel.
VMware haute disponibilité avec pulsations de machine virtuelle	Utilisé pour les défaillances de machine virtuelle.	Non	Utiliser le basculement ASA virtuel pour les défaillances de machine ASA virtuel.
Client Windows autonome VMware vSphere	Utilisé pour déployer les machines virtuelles.	Oui	–
Client Web VMware vSphere	Utilisé pour déployer les machines virtuelles.	Oui	–

Prérequis

Vous pouvez déployer l'ASA virtuel à l'aide du client web VMware vSphere, du client autonome vSphere ou de l'outil OVF. Consultez Compatibilité Cisco Cisco Secure Firewall ASA pour connaître les exigences du système.

Politique de sécurité pour un commutateur standard vSphere

Pour un commutateur vSphere, vous pouvez modifier les politiques de sécurité de couche 2 et appliquer des exceptions aux politiques de sécurité pour les groupes de ports utilisés par les interfaces de l'ASA virtuel. Consultez les paramètres par défaut suivants :

- Mode promiscuité : **Reject** (Refuser)
- Modifications d'adresses MAC : **Accept** (Accepter)

- Transmissions forgées : **Accept** (Accepter)

Vous devrez peut-être modifier ces paramètres pour les configurations ASA virtuel suivantes. Consultez la documentation de vSphere pour en savoir plus.

Tableau 10 : Exceptions à la politique de sécurité du groupe de ports

Exception de sécurité	Mode de pare-feu routé		Mode de pare-feu transparent	
	Aucun basculement	Basculement	Aucun basculement	Basculement
Mode Promiscuous	<any>	<any>	Accepter	Accepter
Modifications d'adresses MAC :	<any>	Accepter	<any>	Accepter
Transmissions forgées	<any>	Accepter	Accepter	Accepter

Décompresser le logiciel ASA virtuel et créer un fichier de configuration de Day 0 (jour 0)

Vous pouvez préparer un fichier de configuration de Day 0 (jour 0) avant de lancer l'ASA virtuel. Ce fichier est un fichier texte qui contient la configuration de l'ASA virtuel à appliquer lors du lancement de l'ASA virtuel. Cette configuration initiale est placée dans un fichier texte nommé « day0-config » dans un répertoire de travail que vous avez choisi, puis manipulée dans un fichier day0.iso qui est monté et lu lors du premier démarrage. Au minimum, le fichier de configuration de Day 0 (jour 0) doit contenir des commandes pour activer l'interface de gestion et configurer le serveur SSH pour l'authentification par clé publique, mais il peut également contenir une configuration ASA complète. Un fichier day0.iso par défaut contenant un fichier day0-config vide est fourni avec la version. Le fichier day0.iso (votre fichier day0.iso personnalisé ou le fichier day0.iso par défaut) doit être disponible lors du premier démarrage.

Avant de commencer

Nous utilisons Linux dans cet exemple, mais il existe des utilitaires similaires pour Windows.

- Pour autoriser automatiquement l'ASA virtuel lors du déploiement initial, placez le jeton d'identité de licence Smart (ID) que vous avez téléchargé à partir de Cisco Smart Software Manager dans un fichier texte nommé « idtoken » dans le même répertoire que le fichier de configuration de Day 0 (jour 0).
- Si vous souhaitez accéder au ASA virtuel à partir du port série de l'hyperviseur au lieu de la console virtuelle VGA, vous devez inclure le paramètre **console serial** (série de la console) dans le fichier de configuration de Day 0 (jour 0) pour utiliser le port série lors du premier démarrage.
- Si vous souhaitez déployer l'ASA virtuel en mode transparent, vous devez utiliser un fichier de configuration ASA connu en cours d'exécution en mode transparent comme fichier de configuration de Dat 0 (jour 0). Cela ne s'applique pas à un fichier de configuration de Day 0 (jour 0) pour un pare-feu avec routeur.

- Consultez les lignes directrices relatives aux fichiers OVF dans Lignes directrices et limites relatives à la licence, à la page 17 pour de plus amples renseignements sur le montage des images ISO sur l'hyperviseur ESXi.

Procédure

Étape 1 Téléchargez le fichier ZIP à partir de Cisco.com et enregistrez-le sur votre disque local :

https://www.cisco.com/go/asa-software

Remarque
Une connexion à Cisco.com et un contrat de service Cisco sont requis.

Étape 2 Décompressez le fichier dans un répertoire de travail. Ne supprimez aucun fichier du répertoire. Les fichiers suivants sont inclus :

- asav-vi.ovf : pour les déploiements vCenter.
- asav-esxi.ovf : pour les déploiements autres que vCenter.
- boot.vmdk : image du disque de démarrage.
- disk0.vmdk : image du disque ASA virtuel.
- day0.iso : ISO contenant un fichier day0-config et éventuellement un fichier idtoken.
- asav-vi.mf : fichier manifeste pour les déploiements vCenter.
- asav-esxi.mf : fichier manifeste pour les déploiements autres que vCenter.

Étape 3 Saisissez la configuration CLI pour l'ASA virtuel dans un fichier texte appelé « day0-config ». Ajoutez des configurations d'interface pour les trois interfaces et toute autre configuration de votre choix.

La première ligne doit commencer par la version de l'ASA. La configuration day0-config doit être une configuration ASA valide. La meilleure façon de générer le fichier day0-config est de copier les parties souhaitées d'une configuration en cours d'exécution à partir d'un ASA ou d'ASA virtuel. L'ordre des lignes dans day0-config est important et doit correspondre à l'ordre observé dans une sortie de commande **show running-config** existante.

Voici deux exemples du fichier day0-config. Le premier exemple montre un fichier day0-config lors du déploiement d'un ASA virtuel avec les interfaces Gigabit Ethernet. Le deuxième exemple montre un fichier day0-config lors du déploiement d'un ASA virtuel avec les interfaces 10 Gigabit Ethernet. Vous utiliseriez ce fichier day0-config pour déployer un ASA virtuel avec des interfaces SR-IOV; consultez Lignes directrices et limites relatives à la licence, à la page 44.

Exemple :

```
ASA Version 9.4.1
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
```

```
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
call-home
http-proxy 10.1.1.1 port 443
license smart
feature tier standard
throughput level 2G
```

Exemple :

```
ASA Version 9.8.1
!
console serial
interface management 0/0
management-only
nameif management
security-level 0
ip address 192.168.0.230 255.255.255.0
!
interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.10.20.10 255.255.255.0
!
route management 0.0.0.0 0.0.0.0 192.168.0.254
!
username cisco password cisco123 privilege 15
!
aaa authentication ssh console LOCAL
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 60
ssh version 2
!
http 0.0.0.0 0.0.0.0 management
!
logging enable
logging timestamp
logging buffer-size 99999
logging buffered debugging
logging trap debugging
!
dns domain-lookup management
DNS server-group DefaultDNS
name-server 64.102.6.247
!
license smart
feature tier standard
throughput level 10G
```

```
!
crypto key generate rsa modulus 2048
```

Étape 4 (Facultatif) Téléchargez le fichier de jeton d'identité de la licence Smart émis par Cisco Smart Software Manager sur votre PC.

Étape 5 (Facultatif) Copiez le jeton d'identification à partir du fichier téléchargé et placez-le dans un fichier texte nommé « idtoken » qui contient uniquement le jeton d'identité.

Le jeton d'identité enregistre automatiquement l'ASA virtuel sur le serveur de licences Smart.

Étape 6 Générez le CD-ROM virtuel en convertissant le fichier texte en fichier ISO :

Exemple :

```
stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size (byptes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

Étape 7 Calculez une nouvelle valeur SHA1 sur Linux pour le fichier day0.iso :

Exemple :

```
openssl dgst -sha1 day0.iso
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66 day0.iso
```

Étape 8 Incluez la nouvelle somme de contrôle dans le fichier asav-vi.mf dans le répertoire de travail et remplacez la valeur day0.iso SHA1 par la nouvelle valeur générée.

Exemple :

```
SHA1(asav-vi.ovf)= de0f1878b8f1260e379ef853db4e790c8e92f2b2
SHA1(disk0.vmdk)= 898b26891cc68fa0c94ebd91532fc450da418b02
SHA1(boot.vmdk)= 6b0000ddebfc38ccc99ac2d4d5dbfb8abfb3d9c4
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66
```

Étape 9 Copiez le fichier day0.iso dans le répertoire où vous avez décompressé le fichier ZIP. Vous remplacerez le fichier day0.iso par défaut (vide).

Lorsqu'une machine virtuelle est déployée à partir de ce répertoire, la configuration du fichier day0.iso nouvellement généré est appliquée.

Déployer l'ASA virtuel à l'aide du client web VMware vSphere

Cette section décrit comment déployer l'ASA virtuel à l'aide du client web VMware vSphere. Le client web nécessite vCenter. Si vous n'avez pas vCenter, consultez Déployer l'ASA virtuel à l'aide du client autonome VMware vSphere et d'une configuration Day0 (Jour0) ou Déployer l'ASA virtuel à l'aide de l'outil OVF et d'une configuration Day0 (Jour0).

- Accéder au client web vSphere et installer le module d'intégration du client, à la page 28
- Déployer l'ASA virtuel à l'aide du client web VMware vSphere, à la page 27

Accéder au client web vSphere et installer le module d'intégration du client

Cette section décrit comment accéder au client web vSphere. Cette section décrit également comment installer le module d'intégration client, qui est requis pour l'accès à la console ASA virtuel. Certaines fonctionnalités client Web (y compris le module d'extension) ne sont pas prises en charge sur Macintosh. Consultez le site Web de VMware pour obtenir des informations complètes sur l'assistance des clients.

Procédure

Étape 1 Lancez le client Web VMware vSphere à partir de votre navigateur :

https://*vCenter_server*:*port*/**vsphere-client/**

Par défaut, le port est 9443.

Étape 2 (Une seule fois) Installez le module d'intégration client pour pouvoir accéder à la console ASA virtuel.

1. Dans l'écran de connexion, téléchargez le module d'extension en cliquant sur **Download the Client Integration Plug-in** (télécharger le module d'intégration de client).
2. Fermez votre navigateur, puis installez le module d'extension à l'aide du programme d'installation.
3. Après l'installation du module d'extension, reconnectez-vous au client Web vSphere.

Étape 3 Saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Login** (connexion), ou cochez la case **Use Windows session authentication** (utiliser l'authentification de session Windows) (Windows uniquement).

Déployer l'ASA virtuel à l'aide du client web VMware vSphere

Pour déployer l'ASA virtuel, utilisez le client web VMware vSphere (ou le client vSphere) et un fichier de modèle dans le format OVF (Open Virtualization Format). Vous utilisez l'assistant de déploiement du modèle OVF dans le client web vSphere pour déployer le paquet Cisco pour l'ASA virtuel. L'assistant analyse le fichier OVF ASA virtuel, crée la machine virtuelle sur laquelle vous allez exécuter l'ASA virtuel et installe le paquet.

La plupart des étapes de l'assistant sont standard pour VMware. Pour en savoir plus sur le modèle de déploiement OVF, consultez l'aide en ligne du client web VMware vSphere.

Avant de commencer

Vous devez avoir au moins un réseau configuré dans vSphere (pour la gestion) avant de déployer l'ASA virtuel.

Procédure

Étape 1 Téléchargez le fichier ZIP ASA virtuel à partir de Cisco.com et enregistrez-le sur votre ordinateur :

http://www.cisco.com/go/asa-software

Remarque
Une connexion à Cisco.com et un contrat de service Cisco sont requis.

Étape 2 Dans le volet **Navigator** (Navigateur) du client web vSphere, cliquez sur **vCenter**.

Étape 3 Cliquez sur **Hosts and Clusters** (Hôtes et grappes).

Étape 4 Faites un clic droit sur le centre de données, la grappe ou l'hôte dans lequel vous souhaitez déployer l'ASA virtuel et choisissez **Déployer le modèle OVF**.
L'assistant de **déploiement du modèle OVF** s'affiche.

Étape 5 Suivez les écrans de l'assistant comme indiqué.

Étape 6 Dans l'écran **Setup networks** (Configuer les réseaux), mappez un réseau à chaque interface ASA virtuel que vous souhaitez utiliser.

Les réseaux ne peuvent pas être en ordre alphabétique. S'il est trop difficile de trouver vos réseaux, vous pouvez modifier les réseaux plus tard à partir de la boîte de dialogue Edit Settings (Modifier les paramètres). Après le déploiement, cliquez avec le bouton droit sur l'instance ASA virtuel et choisissez **Edit Settings** (Modifier les paramètres) pour accéder à la boîte de dialogue **Edit Settings** (Modifier les paramètres). Cependant, cet écran n'affiche pas les ID d'interface ASA virtuel (uniquement les ID d'adaptateur réseau). Consultez la concordance suivante des ID d'adaptateur réseau et des ID d'interface ASA virtuel :

ID d'adaptateur réseau	ID d'interface ASA virtuel
Adaptateur réseau 1	Management 0/0
Adaptateur réseau 2	GigabitEthernet 0/0
Adaptateur réseau 3	GigabitEthernet 0/1
Adaptateur réseau 4	GigabitEthernet 0/2
Adaptateur réseau 5	GigabitEthernet 0/3
Adaptateur réseau 6	GigabitEthernet 0/4
Adaptateur réseau 7	GigabitEthernet 0/5
Adaptateur réseau 8	GigabitEthernet 0/6
Adaptateur réseau 9	GigabitEthernet 0/7
Adaptateur réseau 10	GigabitEthernet 0/8

Vous n'avez pas besoin d'utiliser toutes les interfaces ASA virtuel; cependant, le client Web vSphere vous oblige à attribuer un réseau à toutes les interfaces. Pour les interfaces que vous n'avez pas l'intention d'utiliser, vous pouvez simplement laisser l'interface désactivée dans la configuration ASA virtuel. Après avoir déployé l'ASA virtuel, vous pouvez éventuellement revenir au client web vSphere pour supprimer les interfaces supplémentaires de la boîte de dialogue Edit Settings (Modifier les paramètres). Pour en savoir plus, consultez l'aide en ligne du client web vSphere.

Remarque
Pour les déploiements de basculement/haute disponibilité, GigabitEthernet 0/8 est préconfiguré comme interface de basculement.

Étape 7 Si votre réseau utilise un mandataire HTTP pour l'accès Internet, vous devez configurer l'adresse du mandataire pour les licences Smart dans la zone **Smart Call Home Settings** (Paramètres de Smart Call Home). Ce mandataire est également utilisé pour Smart Call Home en général.

Étape 8 Pour les déploiements de basculement/haute disponibilité, dans l'écran du modèle de personnalisation, configurez les éléments suivants :

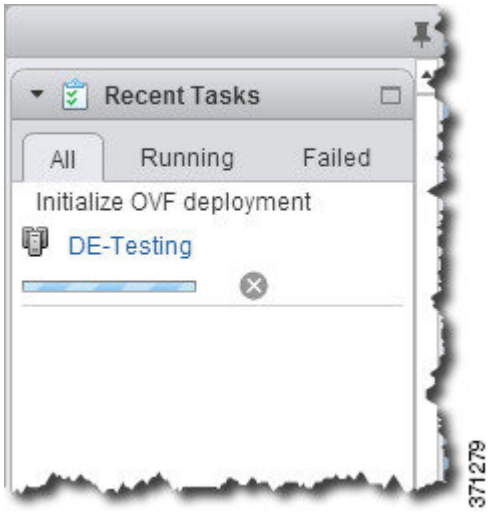
- Précisez l'adresse IP de gestion en veille.

  Lorsque vous configurez vos interfaces, vous devez spécifier une adresse IP active et une adresse IP de secours sur le même réseau. Lorsque l'unité principale bascule, l'unité secondaire adopte les adresses IP et MAC de l'unité principale et commence à transmettre le trafic. L'unité qui est maintenant en état de veille prend le relais des adresses IP et MAC de secours. 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.

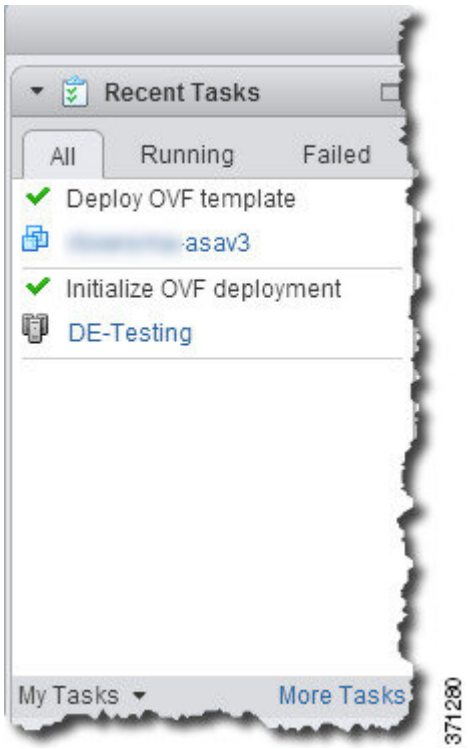
- Configurez les paramètres de liaison de basculement dans la zone **HA Connection Settings** (Paramètres de connexion à haute disponibilité).

  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. GigabitEthernet 0/8 est préconfiguré comme liaison de basculement. Saisissez les adresses IP actives et de secours pour le lien sur le même réseau.

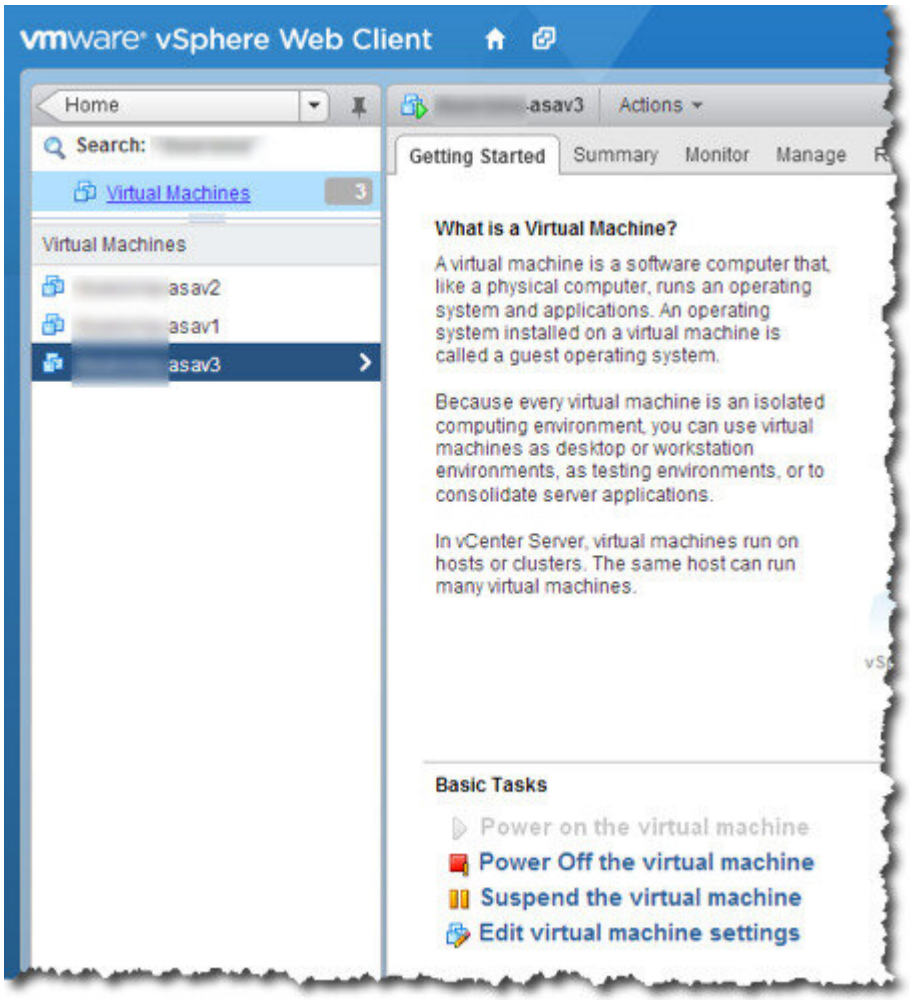
Étape 9 Après avoir terminé l'assistant, le client web vSphere traite la VM; vous pouvez voir l'état « Initalize OVF Deployment » (Initier le déploiement OVF) dans le volet **Recent Tasks** (Tâches récentes) de la zone **Global Information** (Information globale).



Lorsqu'il a terminé, vous voyez l'état d'achèvement du déploiement du modèle OVF.



L'instance de machine ASA virtuel s'affiche ensuite sous le centre de données spécifié dans l'inventaire.



Étape 10 Si la machine ASA virtuel n'est pas encore en cours d'exécution, cliquez sur **Power On the virtual machine** (Mettre la machine virtuelle sous tension).

Attendez que l'ASA virtuel démarre avant d'essayer de vous connecter à ASDM ou à la console. Lorsque l'ASA virtuel démarre pour la première fois, il lit les paramètres fournis par le fichier OVF et les ajoute à la configuration système ASA virtuel. Il reprend ensuite automatiquement le processus de démarrage jusqu'à ce qu'il soit opérationnel. Ce processus de double démarrage se produit uniquement lorsque vous déployez l'ASA virtuel pour la première fois. Pour afficher les messages de démarrage, accédez à la console ASA virtuel en cliquant sur l'onglet **Console**.

Étape 11 Pour les déploiements de basculement/haute disponibilité, répétez cette procédure pour ajouter l'unité secondaire. Consultez les consignes suivantes :

- Définissez le même niveau de débit que l'unité principale.
- Saisissez *exactement les mêmes paramètres d'adresse IP* que pour l'unité principale. Les configurations de démarrage sur les deux unités sont identiques, à l'exception du paramètre identifiant une unité comme principale ou secondaire.

Prochaine étape

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.

Déployer l'ASA virtuel à l'aide du client autonome VMware vSphere et de la configuration Day0 (Jour0).

Pour déployer l'ASA virtuel, utilisez le client VMware vSphere et le fichier de modèle au format OVF (open virtualization format) (asav-vi.ovf pour un déploiement vCenter ou asav-esxi.ovf pour un déploiement non vCenter). Vous utilisez l'assistant de déploiement du modèle OVF dans le client vSphere pour déployer le paquet Cisco pour l'ASA virtuel. L'assistant analyse le fichier OVF ASA virtuel, crée la machine virtuelle sur laquelle vous allez exécuter l'ASA virtuel et installe le paquet.

La plupart des étapes de l'assistant sont standard pour VMware. Pour en savoir plus sur l'assistant de déploiement du modèle OVF, consultez l'aide en ligne du client VMware vSphere.

Avant de commencer

- Vous devez avoir au moins un réseau configuré dans vSphere (pour la gestion) avant de déployer l'ASA virtuel.
- Suivez les étapes dans Décompresser le logiciel ASA virtuel et créer un fichier de configuration de Day 0 (jour 0), à la page 24 pour créer la configuration Day0 (Jour0).

Procédure

Étape 1 Lancez le client VMware vSphere et choisissez **File (Fichier)** > **Deploy OVF Template (Déployer le modèle OVF)**.

L'assistant de déploiement du modèle OVF s'affiche.

Étape 2 Accédez au répertoire de travail où vous avez décompressé le fichier asav-vi.ovf et sélectionnez-le.

Étape 3 Les détails du modèle OVF sont affichés. Passez en revue les écrans suivants. Vous n'avez à modifier aucune configuration si vous choisissez d'utiliser un fichier de configuration Day0 (Jour0) personnalisé.

Étape 4 Un résumé des paramètres de déploiement s'affiche dans le dernier écran. Cliquez sur **Finish** (Terminer) pour déployer la VM.

Étape 5 Mettez l'ASA virtuel sous tension, ouvrez la console VMware et attendez le deuxième démarrage.

Étape 6 Connectez-vous en SSH à l'ASA virtuel et terminez la configuration souhaitée. Si vous n'avez pas toute la configuration souhaitée dans le fichier de configuration Day0 (Jour0), ouvrez une console VMware et terminez la configuration nécessaire.

L'ASA virtuel est maintenant entièrement opérationnel.

Déployer l'ASA virtuel à l'aide de l'outil OVF et de la configuration Day0 (Jour0)

Cette section décrit comment déployer l'ASA virtuel à l'aide de l'outil OVF, qui nécessite un fichier de configuration day0 (jour0).

Avant de commencer

- Le fichier day0.iso est requis lorsque vous déployez l'ASA virtuel à l'aide de l'outil OVF. Vous pouvez utiliser le fichier day0.iso vide par défaut fourni dans le fichier ZIP, ou vous pouvez utiliser un fichier de configuration Day0 (Jour0) personnalisé que vous générez. Consultez Décompresser le logiciel ASA virtuel et créer un fichier de configuration de Day 0 (jour 0), à la page 24 pour créer un fichier de configuration Day0 (Jour0).
- Assurez-vous que l'outil OVF est installé sur un PC Linux ou Windows et qu'il est connecté à votre serveur ESXi cible.

Procédure

Étape 1 Vérifiez que l'outil OVF est installé :

Exemple :

```
linuxprompt# which ovftool
```

Étape 2 Créez un fichier .cmd avec les options de déploiement souhaitées :

Exemple :

```
linuxprompt# cat launch.cmd
ovftool \
--name="asav-941-demo" \
--powerOn \
--deploymentOption=4Core8GB \
--diskMode=thin \
--datastore=datastore1 \
--acceptAllEulas \
--net:Management0-0="Portgroup_Mgmt" \
--net:GigabitEthernet0-1="Portgroup_Inside" \
--net:GigabitEthernet0-0="Portgroup_Outside" \
--prop:HARole=Standalone \
asav-esxi.ovf \
vi://root@10.1.2.3/
```

Étape 3 Exécutez le fichier cmd :

Exemple :

```
linuxprompt# ./launch.cmd
```

L'ASA virtuel est activé; attendez le deuxième démarrage.

Étape 4 Connectez-vous en SSH à l'ASA virtuel pour terminer la configuration au besoin. Si une configuration supplémentaire est requise, ouvrez la console VMware sur l'ASA virtuel et appliquez la configuration nécessaire.

L'ASA virtuel est maintenant entièrement opérationnel.

Accéder à la console ASA virtuel

Dans certains cas, avec ASDM, vous devrez peut-être utiliser l'interface de ligne de commande pour le dépannage. Par défaut, vous pouvez accéder à la console VMware vSphere intégrée. Vous pouvez également configurer une console série de réseau, qui a de meilleures capacités, notamment pour copier et coller.

- Utiliser la console VMware vSphere
- Configurer un port de console de série de réseau

Remarque Si vous déployez l'ASA virtuel à l'aide d'un fichier de configuration de Day0 (Jour0), vous pouvez inclure le paramètre **console serial** (série de la console) dans le fichier de configuration pour utiliser le port série sur le premier démarrage au lieu de la console virtuelle VGA; voir Décompresser le logiciel ASA virtuel et créer un fichier de configuration de Day 0 (jour 0), à la page 24.

Utiliser la console VMware vSphere

Pour la configuration initiale ou le dépannage, accédez à l'interface de ligne de commande à partir de la console virtuelle fournie par l'intermédiaire du client web VMware vSphere. Vous pourrez configurer ultérieurement l'accès à distance à l'interface de ligne de commande pour Telnet ou SSH.

Avant de commencer

Pour le client web vSphere, installez le module d'intégration de client, qui est requis pour l'accès à la console ASA virtuel.

Procédure

Étape 1 Dans le client web VMware vSphere, cliquez avec le bouton droit sur l'instance ASA virtuel dans l'inventaire et choisissez **Open Console** (Ouvrir la console). Vous pouvez également cliquer sur **Launch Console** (Lancer la console) sous l'onglet Summary (Résumé).

Étape 2 Cliquez dans la console et appuyez sur **Enter** (Entrée). Remarque : appuyez sur **Ctrl + Alt** pour libérer le curseur.

Si l'ASA virtuel démarre toujours, des messages de démarrage s'affichent.

Lorsque l'ASA virtuel démarre pour la première fois, il lit les paramètres fournis par le fichier OVF et les ajoute à la configuration système ASA virtuel. Il reprend ensuite automatiquement le processus de démarrage jusqu'à ce qu'il soit opérationnel. Ce processus de double démarrage se produit uniquement lorsque vous déployez l'ASA virtuel pour la première fois.

Remarque

Jusqu'à ce que vous installiez une licence, le débit est limité à 100 kbit/s afin que vous puissiez effectuer des tests de connectivité préalables. Une licence est requise pour le fonctionnement normal. Vous voyez également les messages suivants répétés sur la console jusqu'à ce que vous installiez une licence :

```
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.
```

L'invite suivante s'affiche :

```
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.

Exemple :

```
ciscoasa> enable
```

Le message suivant s'affiche :

```
Password:
```

Étape 4 Appuyez sur la touche **Enter** (Entrée) pour continuer. Par défaut, le champ du mot de passe est vide. Si vous avez déjà défini un mot de passe d'activation, saisissez-le au lieu d'appuyer sur Enter (Entrée).

L'invite passe à :

```
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 5 Accédez au mode de configuration globale :

```
ciscoasa# configure terminal
```

L'invite change comme suit :

```
ciscoasa(config)#
```

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

Configurer un port de console de série de réseau

Pour une meilleure expérience de la console, vous pouvez configurer un port série réseau individuellement ou relié à un concentrateur de port série virtuel (vSPC) pour l'accès à la console. Consultez la documentation de VMware vSphere pour en savoir plus sur chaque méthode. Sur l'ASA virtuel, vous devez envoyer la sortie de la console à un port série plutôt qu'à la console virtuelle. Cette procédure décrit comment activer la console de port série.

Procédure

Étape 1 Configurez un port série réseau dans VMware vSphere. Consultez la documentation de VMware vSphere.

Étape 2 Sur l'ASA virtuel, créez un fichier appelé « use_ttyS0 » dans le répertoire racine de disk0. Ce fichier n'a pas besoin d'avoir du contenu; il doit simplement exister à cet emplacement :

disk0 :/use_ttyS0

- À partir d'ASDM, vous pouvez charger un fichier texte vide portant ce nom à l'aide de la boîte de dialogue **Tools (Outils)** > **File Management (Gestion des fichiers)**.
- Au niveau de la console vSphere, vous pouvez copier un fichier existant (n'importe quel fichier) dans le système de fichiers sous le nouveau nom. Par exemple :

```
ciscoasa(config)# cd coredumpinfo
ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
```

Étape 3 Rechargez l'ASA virtuel.

- Dans ASDM, choisissez **Tools (Outils)** > **System Reload (Recharger le système)**.
- Dans la console vSphere, saisissez **reload** (recharger).

  L'ASA virtuel arrête l'envoi à la console vSphere et l'envoie plutôt à la console série.

Étape 4 Utilisez Telnet à l'adresse IP de l'hôte vSphere et au numéro de port que vous avez spécifié lorsque vous avez ajouté le port série; ou utilisez Telnet à l'adresse IP et au port vSPC.

Mettre à niveau la licence vCPU ou débit

L'ASA virtuel utilise une licence débit, qui affecte le nombre de vCPU que vous pouvez utiliser.

Si vous souhaitez augmenter (ou diminuer) le nombre de vCPU pour votre ASA virtuel, vous pouvez demander une nouvelle licence, appliquer la nouvelle licence et modifier les propriétés de la machine virtuelle dans VMware pour qu'elles correspondent aux nouvelles valeurs.

Remarque Les vCPU attribuées doivent correspondre à la licence CPU ASA virtuel ou à la licence débit. La mémoire RAM doit également être de taille appropriée pour les vCPU. Lors de la mise à niveau ou de la rétrogradation, assurez-vous de suivre cette procédure et de rapprocher la licence et les vCPU immédiatement. L'ASA virtuel ne fonctionne pas correctement en cas d'incompatibilité persistante.

Procédure

Étape 1 Demandez une nouvelle licence.

Étape 2 Appliquez la nouvelle licence. Pour les paires de basculement, appliquez de nouvelles licences aux deux unités.

Étape 3 Effectuez l'une des opérations suivantes, selon que vous utilisez le basculement, ou non :

- Basculement : dans le client Web vSphere, éteignez l'ASA virtuel en mode veille. Par exemple, cliquez sur l'ASA virtuel, puis sur **Power Off the virtual machine** (éteindre la machine virtuelle), ou cliquez avec le bouton droit sur l'ASA virtuel et choisissez **Shut Down Guest OS** (arrêter le système d'exploitation invité).
- Aucun basculement : dans le client Web vSphere, éteignez l'ASA virtuel. Par exemple, cliquez sur l'ASA virtuel, puis sur **Power Off the virtual machine** (éteindre la machine virtuelle), ou cliquez avec le bouton droit sur l'ASA virtuel et choisissez **Shut Down Guest OS** (arrêter le système d'exploitation invité).

Étape 4 Cliquez sur l'ASA virtuel, puis sur **Edit Virtual machine settings** (modifier les paramètres de la machine virtuelle) (ou cliquez avec le bouton droit sur l'ASA virtuel et choisissez **Edit Settings** (modifier les paramètres).

La boîte de dialogue **Edit Settings** (modifier les paramètres) s'affiche.

Étape 5 Reportez-vous aux exigences de CPU et de mémoire dans Gestion des licences pour l'ASA virtuel, à la page 1 pour déterminer les valeurs correctes pour la nouvelle licence vCPU.

Étape 6 Sous l'onglet **Virtual Hardware** (matériel virtuel), pour le **CPU**, choisissez la nouvelle valeur dans la liste déroulante.

Étape 7 Pour **Memory** (mémoire), entrez la nouvelle valeur de la mémoire RAM.

Étape 8 Cliquez sur **OK**.

Étape 9 Mettez l'ASA virtuel. Par exemple, cliquez sur **Power On the Virtual Machine** (mettez la machine virtuelle sous tension).

Étape 10 Pour les paires de basculement :

1. Ouvrez une console à l'unité active ou lancez ASDM sur l'unité active.
2. Une fois que l'unité en mode veille a terminé de démarrer, basculez vers l'unité en mode veille :
   - ASDM : choisissez **Monitoring (supervision)** > **Properties (propriétés)** > **Faillover (basculement)** > **Status (état)**, et cliquez sur **Make Standby** (mettre en veille).
   - Interface de ligne de commande : **failover active**
3. Répétez les étapes 3 à 9 pour l'unité active.

Prochaine étape

Consultez la Gestion des licences pour l'ASA virtuel, à la page 1 pour de plus amples renseignements.

Réglage de la performance

Amélioration de la performance pour les configurations ESXi

Vous pouvez améliorer la performance d'un ASA virtuel dans l'environnement ESXi en réglant les paramètres de configuration du CPU de l'hôte ESXi. L'option Scheduling Affinity (planification de l'affinité) vous permet de contrôler la répartition des CPU des machines virtuelles sur les cœurs physiques de l'hôte (et sur les hyperthreads si l'hyperthreading est activé). En utilisant cette fonctionnalité, vous pouvez affecter chaque machine virtuelle aux processeurs de l'ensemble d'affinité spécifié.

Consultez les documents VMware suivants pour plus d'informations :

- Le chapitre *Administration des ressources du CPU* de Gestion des ressources de vSphere.
- Bonnes pratiques en matière de performance pour VMware vSphere.
- L'aide en ligne du client vSphere.

Lignes directrices NUMA

L'accès mémoire non uniforme (NUMA, Non-Uniform Memory Access) est une architecture de mémoire partagée qui décrit le placement des modules de mémoire principaux en ce qui concerne les processeurs dans un système multiprocesseur. Lorsqu'un processeur accède à la mémoire qui ne se trouve pas dans son propre nœud (mémoire distante), les données doivent être transférées sur la connexion NUMA à un débit plus lent qu'il ne le serait lors de l'accès à la mémoire locale.

L'architecture du serveur x86 est composée de plusieurs connecteurs et de plusieurs cœurs dans un connecteur. Chaque connecteur CPU, ainsi que sa mémoire et son entrée-sortie, est appelé nœud NUMA. Pour lire efficacement les paquets à partir de la mémoire, les applications invitées et les périphériques associés (comme la carte d'interface réseau) doivent résider sur le même nœud.

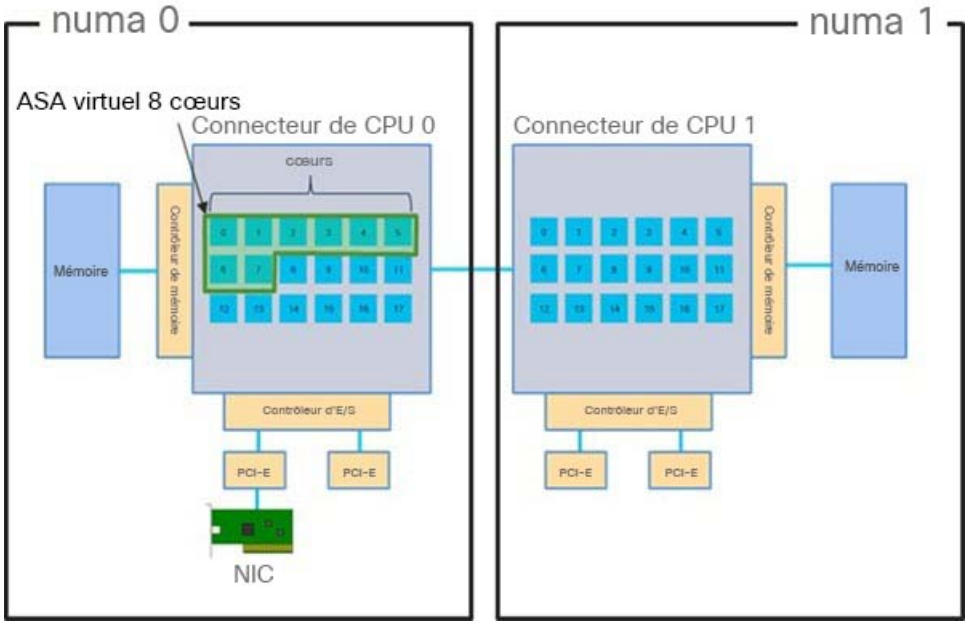
Pour une performance ASA virtuel optimale :

- La machine ASA virtuel doit fonctionner sur un seul nœud numa. Si un seul ASA virtuel est déployé de sorte qu'il fonctionne sur deux connecteurs, la performance sera considérablement réduite.
- Un ASA virtuel à 8 cœurs (Illustration 1 : Exemple d'architecture NUMA à 8 cœurs, à la page 40) exige que chaque connecteur du CPU hôte ait au moins 8 cœurs par connecteur. Il faut tenir compte des autres machines virtuelles en cours d'exécution sur le serveur.
- Un ASA virtuel [ ] ([] 16 cœurs (Illustration 2 : Exemple d'architecture NUMA ASA virtuel à 16 cœurs, à la page 40) exige que chaque connecteur du CPU hôte ait un minimum de 16 cœurs par connecteur. Il faut tenir compte des autres machines virtuelles en cours d'exécution sur le serveur.
- La carte réseau (NIC) doit se trouver sur le même nœud NUMA que la machine ASA virtuel.

Remarque L'ASA virtuel ne prend pas en charge les nœuds multiples d'‘accès à la mémoire non uniforme (numéro) et plusieurs connecteurs de CPU pour les cœurs physiques.

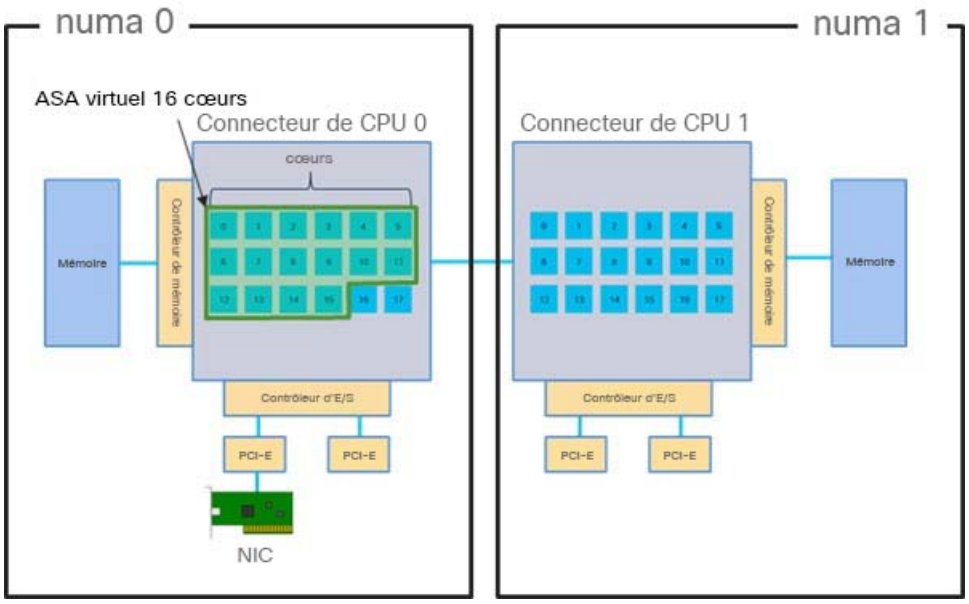
La figure suivante montre un serveur avec deux connecteurs pour CPU, chaque CPU ayant 18 cœurs. L'ASA virtuel à 8 cœurs exige que chaque connecteur du CPU hôte ait au moins 8 cœurs.

Illustration 1 : Exemple d'architecture NUMA à 8 cœurs



La figure suivante montre un serveur avec deux connecteurs pour CPU, chaque CPU ayant 18 cœurs. L'ASA virtuel à 16 cœurs exige que chaque connecteur du CPU hôte ait au moins 16 cœurs.

Illustration 2 : Exemple d'architecture NUMA ASA virtuel à 16 cœurs



Vous trouverez plus de renseignements sur l'utilisation des systèmes NEMA avec ESXi dans le document VMware *Gestion des ressources de vSphere* pour votre version de VMware ESXi. Pour vérifier les versions les plus récentes de ce document et d'autres documents pertinents, consultez la page http://www.vmware.com/support/pubs

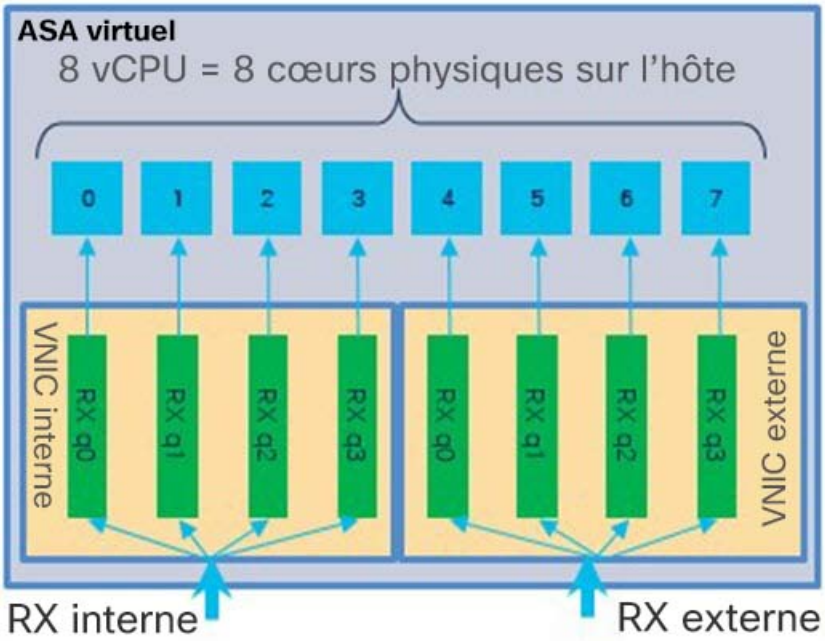
Files d'attente RX multiples pour le dimensionnement de la réception (RSS).

L'ASA virtuel prend en charge le dimensionnement de la réception (RSS), qui est une technologie utilisée par les adaptateurs réseau pour distribuer le trafic de réception réseau entre plusieurs cœurs de processeur. Pour un débit maximal, chaque vCPU (cœur) doit avoir sa propre file d'attente NIC RX. Notez qu'un déploiement typique de réseau privé virtuel (VPN) d'accès à distance peut utiliser une seule paire d'interfaces interne/externe.

Important La version 9.13(1) ou ultérieure d'ASA virtuel est nécessaire pour utiliser plusieurs files d'attente RX.

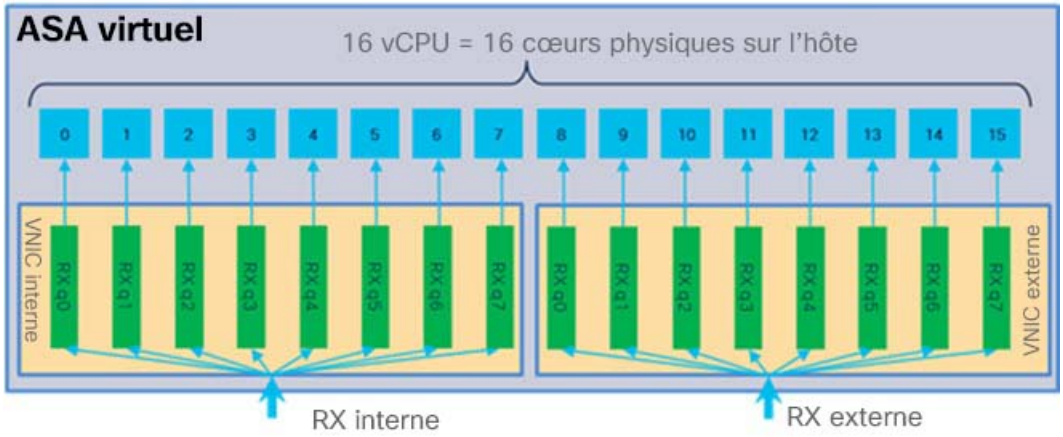
Pour une machine virtuelle à 8 cœurs avec une paire d'interfaces interne/externe, chaque interface aura 4 files d'attente RX, comme indiqué dans Illustration 3 : Files d'attente RX RSS à 8 cœurs ASA virtuel , à la page 41.

Illustration 3 : Files d'attente RX RSS à 8 cœurs ASA virtuel



Pour une machine virtuelle à 16 cœurs avec une paire d'interfaces interne/externe, chaque interface aura 8 files d'attente RX, comme indiqué dans Illustration 4 : Files d'attente RX RSS à 16 cœurs ASA virtuel, à la page 42.

Illustration 4 : Files d'attente RX RSS à 16 cœurs ASA virtuel



Le tableau suivant présente les vNIC de l'ASA virtuel pour VMware et le nombre de files d'attente RX prises en charge. Consultez vNIC recommandées, à la page 18 pour obtenir des descriptions des vNIC prises en charge.

Tableau 11 : NIC/vNIC recommandées par VMware

Carte NIC	Pilote vNIC	Technologie de pilote	Nombre de files d'attente RX	Rendement
x710*	i40e	PCI Passthrough (transmission directe de PCI)	8 max	PCI Passthrough (transmission directe de PCI) offre la plus haute performance des cartes réseau (NIC) testées. En mode de transmission directe, la carte d'interface réseau est dédiée au ASA virtuel et ne constitue pas un choix optimal pour virtuel.
	i40evf	SR-IOV	4	Le SR-IOV avec la carte réseau x710 a un débit inférieur (environ 30 %) à PCI Passthrough (transmission directe de PCI). i40evf sur VMware a un maximum de 4 files d'attente RX par i40evf . 8 files d'attente RX sont nécessaires pour obtenir un débit maximal sur une machine virtuelle à 16 cœurs.
x520	ixgbe-vf	SR-IOV	2	—
	ixgbe	PCI Passthrough (transmission directe de PCI)	6	Le pilote ixgbe (en mode PCI Passthrough) dispose de 6 files d'attente RX. La performance est similaire à celle d'i40evf (SR-IOV).
S. O.	vmxnet3	Paravirtualisation	8 max	Non recommandé pour ASAv100.

Carte NIC	Pilote vNIC	Technologie de pilote	Nombre de files d'attente RX	Rendement
S. O.	e1000	Non recommandé par VMware.		
* L'ASA virtuel n'est pas compatible avec le pilote d'hôte i40en de 1.9.5 pour la carte réseau x710. Les versions de pilote plus anciennes ou plus récentes fonctionneront. Consultez Identifier les versions des pilotes NIC et du micrologiciel, à la page 43 pour en savoir plus sur les commandes ESXCLI pour identifier ou vérifier les versions du pilote NIC et du micrologiciel.				

Identifier les versions des pilotes NIC et du micrologiciel

Si vous devez identifier ou vérifier les informations relatives à la version de votre micrologiciel et de votre pilote, il est possible de trouver ces données à l'aide des commandes ESXCLI.

- Pour obtenir une liste des cartes réseau (NIC) installées, connectez-vous avec le protocole SSH à l'hôte pertinent et exécutez la commande `esxcli network nic list`. Cette commande devrait vous fournir une liste des périphériques et des informations générales.
- Après avoir obtenu une liste des cartes réseau (NIC) installées, vous pouvez extraire des informations détaillées sur la configuration. Exécutez la commande `esxcli network nic get` en précisant le nom de la carte d'interface réseau (NIC) nécessaire : `esxcli network nic get -n<nic name>`.

Remarque Les informations générales sur l'adaptateur de réseau peuvent également être consultées à partir du client VMware vSphere. L'adaptateur et le pilote se trouvent sous **Physical Adapters** (adaptateurs physiques) dans l'onglet **Configure** (configurer).

Provisionnement d'interface SR-IOV

SR-IOV permet à plusieurs machines virtuelles de partager un seul adaptateur réseau PCIe à l'intérieur d'un hôte. SR-IOV définit ces fonctions :

- Fonction physique (PF) : les PF sont des fonctions PCIe complètes qui comprennent les capacités SR-IOV. Celles-ci s'affichent comme des cartes réseau (NIC) statiques normales sur le serveur hôte.
- Fonction virtuelle (VF) : les VF sont des fonctions PCIe allégées qui aident au transfert de données. Une VF est dérivée d'une PF et gérée par l'intermédiaire d'une PF.

Les VF peuvent fournir une connectivité allant jusqu'à 10 Gbit/s à la machine ASA virtuel dans une structure de système d'exploitation virtualisé. Cette section explique comment configurer les VF dans un environnement KVM. La prise en charge de SR-IOV sur l'ASA virtuel est expliquée dans ASA virtuel et provisionnement de l'interface SR-IOV, à la page 12.

Sur ASAv5 et ASAv10, le pilote VMXNET3 est fortement recommandé pour une performance optimale. De plus, l'interface SR-IOV, lorsqu'elle est utilisée en combinaison (mélange d'interfaces), améliore la performance du réseau avec ASA virtuel, en particulier avec l'allocation de plus de cœurs et de ressources pour le processeur (CPU).

Lignes directrices et limites relatives à la licence

Lignes directrices relatives aux interfaces SR-IOV

VMware vSphere 5.1 et les versions ultérieures prennent en charge SR-IOV dans un environnement avec des configurations spécifiques uniquement. Certaines fonctionnalités de vSphere ne sont pas opérationnelles lorsque SR-IOV est activé.

En plus des exigences système pour l'ASA virtuel et SR-IOV comme décrit dans Lignes directrices et limites des interfaces SR-IOV, à la page 13, vous devez passer en revue les configurations prises en charge pour l'utilisation de SR-IOV dans la documentation de VMware pour en savoir plus sur les exigences, les cartes réseau prises en charge, la disponibilité des fonctionnalités et les exigences de mise à niveau pour VMware et SR-IOV.

ASA virtuel sur VMware à l'aide de l'interface SR-IOV prend en charge le mélange de types d'interfaces. Vous pouvez utiliser SR-IOV ou VMXNET3 pour l'interface de gestion et SR-IOV pour l'interface de données.

Cette section montre diverses étapes d'installation et de configuration pour le provisionnement des interfaces SR-IOV sur un système VMware. Les renseignements figurant dans cette section ont été créés à partir de périphériques dans un environnement de laboratoire spécifique, en utilisant VMware ESXi 6.0 et le client web vSphere, un serveur Cisco série UCS C et un adaptateur de serveur Ethernet Intel X520 - DA2.

Limites des interfaces SR-IOV

Lorsque l'ASA virtuel est démarré, sachez que les interfaces SR-IOV peuvent s'afficher dans l'ordre inverse de celui présenté dans ESXi. Cela pourrait entraîner des erreurs de configuration d'interface qui entraîneront un manque de connectivité réseau pour une machine ASA virtuel particulière.

Mise en garde Il est important de vérifier le mappage de l'interface avant de commencer à configurer les interfaces réseau SR-IOV sur l'ASA virtuel. Cela garantit que la configuration de l'interface réseau s'appliquera à la bonne interface d'adresse MAC physique sur l'hôte de machine virtuelle.

Après le démarrage du ASA virtuel, vous pouvez confirmer quelle adresse MAC est mappée à quelle interface. Utilisez la commande **show interface** (afficher l'interface) pour afficher des renseignements détaillés sur l'interface, y compris l'adresse MAC d'une interface. Comparez l'adresse MAC avec les résultats de la commande **show kernel ifconfig** pour confirmer l'affectation d'interface correcte.

Vérifier le BIOS de l'hôte ESXi

Pour déployer l'ASA virtuel avec les interfaces SR-IOV sur VMware, la virtualisation doit être prise en charge et activée. VMware fournit plusieurs méthodes pour vérifier la prise en charge de la virtualisation, y compris leur Guide de compatibilité en ligne pour la prise en charge de SR-IOV et un programme utilitaire d'identification de CPU téléchargeable qui détecte si la virtualisation est activée ou désactivée.

Vous pouvez également déterminer si la virtualisation est activée dans le BIOS en vous connectant à l'hôte ESXi.

Procédure

Étape 1 Connectez-vous à l'interface Shell ESXi en utilisant l'une des méthodes suivantes :

- Si vous avez un accès direct à l'hôte, appuyez sur Alt+F2 pour ouvrir la page de connexion sur la console physique de la machine.
- Si vous vous connectez à l'hôte à distance, utilisez le protocole SSH ou une autre connexion de console distante pour démarrer une session sur l'hôte.

Étape 2 Saisissez un nom d'utilisateur et un mot de passe reconnus par l'hôte.

Étape 3 Exécutez la commande suivante :

Exemple :

```
esxcfg-info|grep "\----\HV Support"
```

Le résultat de la commande HV Support indique le type de prise en charge d'hyperviseur disponible. Voici les descriptions des valeurs possibles :

0 – VT/AMD-V indique que la prise en charge n'est pas disponible pour ce matériel.

1 – VT/AMD-V indique que VT ou AMD-V peut être disponible, mais qu'il n'est pas pris en charge par ce matériel.

2 – VT/AMD-V indique que VT ou AMD-V est disponible, mais n'est actuellement pas activé dans le BIOS.

3 – VT/AMD-V indique que VT ou AMD-V est activé dans le BIOS et peut être utilisé.

Exemple :

```
~ # esxcfg-info|grep "\----\HV Support"
        |----HV Support.........................3
```

La valeur 3 indique que la virtualisation est prise en charge et activée.

Prochaine étape

- Activez SR-IOV sur l'adaptateur physique de l'hôte.

Activer SR-IOV sur l'adaptateur physique de l'hôte

Utilisez le client web vSphere pour activer SR-IOV et définir le nombre de fonctions virtuelles sur votre hôte. Vous ne pouvez pas connecter des machines virtuelles aux fonctions virtuelles avant de le faire.

Avant de commencer

- Assurez-vous d'avoir installé une carte d'interface réseau (NIC) compatible avec SR-IOV; voir Cartes réseau (NIC) prises en charge pour SR-IOV, à la page 14.

Procédure

Étape 1 Dans le client web vSphere, accédez à l'hôte ESXi sur lequel vous souhaitez activer SR-IOV.

Étape 2 Dans l'onglet **Manage** (Gérer), cliquez sur **Networking** (Mise en réseau) et sélectionnez **Physical Adapters** (Adaptateurs physiques).

Vous pouvez consulter la propriété SR-IOV pour voir si un adaptateur physique prend en charge SR-IOV.

Étape 3 Sélectionnez l'adaptateur physique et cliquez sur **Edit Adapter Settings** (Modifier les paramètres de l'adaptateur).

Étape 4 Sous SR-IOV, sélectionnez **Enabled** (Activé) dans le menu déroulant **Status** (État).

Étape 5 Dans la zone de texte **Number of virtual functions** (Nombre de fonctions virtuelles), saisissez le nombre de fonctions virtuelles que vous souhaitez configurer pour l'adaptateur.

Remarque
Pour ASAv50, nous vous recommandons de **NE PAS** utiliser plus d'une VF par interface. Une dégradation des performances est susceptible de se produire si vous partagez l'interface physique avec plusieurs fonctions virtuelles.

Étape 6 Cliquez sur **OK**.

Étape 7 Redémarrez l'hôte ESXi.

Les fonctions virtuelles deviennent actives sur le port NIC représenté par l'entrée d'adaptateur physique. Elles apparaissent dans la liste PCI Devices (Appareils PCI) de l'onglet **Settings** (Paramètres) de l'hôte.

Prochaine étape

- Créez un vSwitch standard pour gérer les fonctions et les configurations SR-IOV.

Créer un commutateur vSphere

Créez un commutateur vSphere pour gérer les interfaces SR-IOV.

Procédure

Étape 1 Dans le client web vSphere, accédez à l'hôte ESXi.

Étape 2 Sous **Manage** (Gérer), sélectionnez **Networking** (Mise en réseau), puis **Virtual switches** (Commutateurs virtuels).

Étape 3 Cliquez sur l'icône **Add host networking** (Ajouter la mise en réseau des hôtes), qui est l'icône en forme de globe vert avec le signe plus (+).

Étape 4 Sélectionnez un type de connexion **Virtual Machine Port Group for a Standard Switch** (Groupe de ports de machines virtuelles pour un commutateur standard) et cliquez sur **Next** (Suivant).

Étape 5 Sélectionnez **New standard switch** (Nouveau commutateur standard) et cliquez sur **Next** (Suivant).

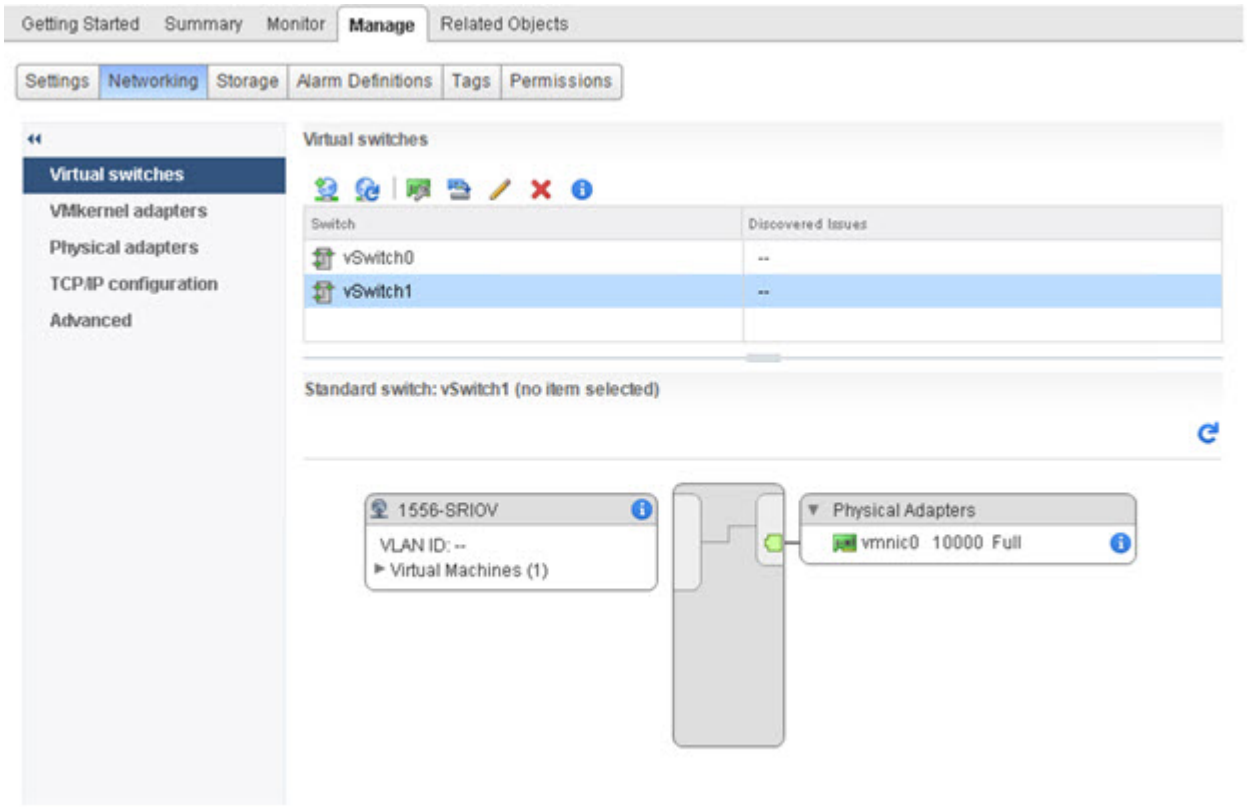
Étape 6 Ajoutez des adaptateurs réseau physiques au nouveau commutateur standard.

a) Sous Affected Adapters (Adaptateurs attribués), cliquez sur le signe plus vert (+) pour **Add Adapters** (Ajouter des adaptateurs).
b) Sélectionnez l'interface réseau correspondante pour SR-IOV dans la liste. Par exemple, Intel(R) 82599, 10 Gigabit, connexion réseau à double port.
c) Dans le menu déroulant **Failover order group** (Groupe de commandes de basculement), sélectionnez parmi les **Active adapters** (Adaptateurs actifs).
d) Cliquez sur **OK**.

Étape 7 Saisissez une **Network label** (Étiquette de réseau) pour le vSwitch SR-IOV et cliquez sur **Next** (Suivant).

Étape 8 Passez en revue vos sélections sur la page **Ready to complete** (Prêt à terminer), puis cliquez sur **Finish** (Terminer).

Illustration 5 : Nouveau vSwitch avec une interface SR-IOV associée



Prochaine étape

- Examinez le niveau de compatibilité de votre machine virtuelle.

Mettre à niveau le niveau de compatibilité des machines virtuelles

Le niveau de compatibilité détermine le matériel virtuel disponible pour la machine virtuelle, qui correspond au matériel physique disponible sur la machine hôte. La machine ASA virtuel doit être au niveau matériel 10 ou supérieur. Cela exposera la fonctionnalité de transmission directe SR-IOV à l'ASA virtuel. Cette procédure met immédiatement à niveau l'ASA virtuel vers la dernière version de matériel virtuel prise en charge.

Pour en savoir plus sur les versions matérielles et la compatibilité des machines virtuelles, consultez la documentation d'administration de la machine virtuelle de vSphere.

Procédure

Étape 1 Connectez-vous au serveur vCenter à partir du client Web vSphere.

Étape 2 Localisez la machine ASA virtuel que vous souhaitez modifier.

a) Sélectionnez un centre de données, un dossier, une grappe, un ensemble de ressources ou un hôte et cliquez sur l'onglet **Related Objects** (objets associés).

b) Cliquez sur **Virtual Machines** (machines virtuelles) et sélectionnez la machine ASA virtuel dans la liste.

Étape 3 Mettez la machine virtuel sélectionnée sous tension.

Étape 4 Faites un clic droit sur l'ASA virtuel et sélectionnez **Actions** > **All vCenter Actions (toutes les actions de centre virtuel)** > **Compatibility (compatibilité)** > **Upgrade VM Compatibility (mettre à niveau la compatibilité de la machine virtuelle)**.

Étape 5 Cliquez sur **Yes** (Oui) pour confirmer le mise à niveau.

Étape 6 Choisissez l'option **ESXi 5.5 and later** (ESXi 5.5 ou ultérieure) pour la compatibilité des machines virtuelles.

Étape 7 (Facultatif) Sélectionnez **Only upgrade after normal guest OS shutdown** (Mettre à niveau seulement après l'arrêt normal du système d'exploitation invité).

La machine virtuelle sélectionnée est mise à niveau vers la version matérielle correspondante pour le paramètre de compatibilité que vous avez choisi, et la nouvelle version matérielle est mise à jour dans l'onglet Summary (sommaire) de la machine virtuelle.

Prochaine étape

- Associez l'ASA virtuel à une fonction virtuelle par l'intermédiaire d'un adaptateur de réseau de transmission directe SR-IOV.

Attribuer la carte NIC SR-IOV à l'ASA virtuel

Pour vous assurer que la machine ASA virtuel et la carte réseau physique peuvent échanger des données, vous devez associer l'ASA virtuel à une ou plusieurs fonctions virtuelles en tant qu'adaptateurs réseau de transmission directe SR-IOV. La procédure suivante explique comment affecter la carte réseau SR-IOV à la machine ASA virtuel à l'aide du client web vSphere.

Procédure

Étape 1 Connectez-vous au serveur vCenter à partir du client web vSphere.

Étape 2 Localisez la machine ASA virtuel que vous souhaitez modifier.

a) Sélectionnez un centre de données, un dossier, une grappe, un ensemble de ressources ou un hôte et cliquez sur l'onglet **Related Objects** (Objets associés).

b) Cliquez sur **Virtual Machines** (Machines virtuelles) et sélectionnez la machine ASA virtuel dans la liste.

Étape 3 Dans l'onglet **Manage** (Gérer) de la machine virtuelle, sélectionnez **Settings (Paramètres)** > **VM Hardware (Matériel VM)**.

Étape 4 Cliquez sur **Edit** (Modifier) et sélectionnez l'onglet **Virtual Hardware** (Matériel virtuel).

Étape 5 Dans le menu déroulant **New device** (Nouveau périphérique), sélectionnez **Network** (Réseau) et cliquez sur **Add** (Ajouter).

Une interface **New Network** (Nouveau réseau) s'affiche.

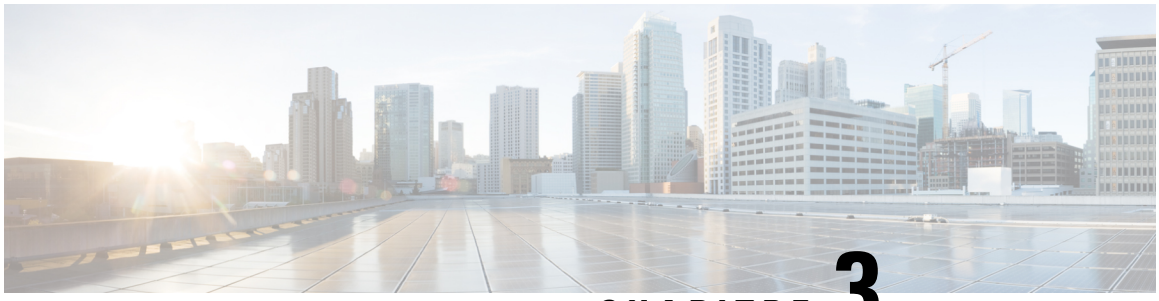
Étape 6 Développez la section **New Network** (Nouveau réseau) et sélectionnez une option SR-IOV disponible.

Étape 7 Dans le menu déroulant **Adapter Type** (Type d'adaptateur), sélectionnez **SR-IOV passthrough** (Transmission directe SR-IOV).

Étape 8 Dans le menu déroulant **Physical Function** (Fonction physique), sélectionnez l'adaptateur physique qui correspond à l'adaptateur de machine virtuelle de transmission directe.

Étape 9 Mettez l'ordinateur virtuel sous tension.

Lorsque vous mettez la machine virtuelle sous tension, l'hôte ESXi sélectionne une fonction virtuelle libre dans l'adaptateur physique et la mappe à l'adaptateur de transmission directe SR-IOV. L'hôte valide toutes les propriétés de l'adaptateur de machine virtuelle et de la fonction virtuelle sous-jacente.



CHAPITRE 3

Déployer l'ASA virtuel à l'aide de KVM

Vous pouvez déployer l'ASA virtuel sur n'importe quel périphérique CPU de *classe de serveur* x86 capable d'exécuter la machine virtuelle basée sur le noyau (KVM).

Important La mémoire minimale requise pour l'ASA virtuel est de 2 Go. Si votre ASA virtuel actuel fonctionne avec moins de 2 Go de mémoire, vous ne pouvez pas effectuer de mise à niveau vers la version 9.13(1)+ à partir d'une version antérieure sans augmenter la mémoire de votre machine ASA virtuel. Vous pouvez également redéployer une nouvelle machine ASA virtuel avec la dernière version.

- Lignes directrices et limites relatives à la licence, à la page 51
- Aperçu, à la page 54
- Prérequis, à la page 54
- Préparer le fichier de configuration Day0 (Jour0), à la page 55
- Préparer les fichiers XML de pont virtuel, à la page 57
- Déployer l'ASA virtuel, à la page 58
- Réglage de la performance, à la page 59
- Utilisation et rapport d'utilisation du processeur (CPU), à la page 71

Lignes directrices et limites relatives à la licence

Le matériel spécifique utilisé pour les déploiements d'ASA virtuel peut varier en fonction du nombre d'instances déployées et des exigences d'utilisation. Chaque appliance virtuelle que vous créez nécessite une allocation minimale de ressources (mémoire, nombre de CPU et espace disque) sur la machine hôte.

Important L'ASA virtuel est déployé avec une taille de stockage sur disque de 8 Go. Il est impossible de modifier l'allocation des ressources de l'espace disque.

Remarque À partir de la version 9.16.x d'ASA virtuel, lorsque vous rétrogradez d'ASAv100, dont la configuration de l'appareil est de 16 vCPU et de 32 Go de RAM, à ASAv10, vous devez configurer l'appareil avec 1 vCPU et 4 Go de RAM.

Passez en revue les lignes directrices et les limites suivantes avant de déployer l'ASA virtuel.

Configuration système requise pour ASA virtuel sur KVM

Assurez-vous de vous conformer aux caractéristiques ci-dessous pour assurer des performances optimales. Les conditions requises par l'ASA virtuel sont les suivantes :

- Le CPU de l'hôte doit être un processeur Intel ou AMD de *classe de serveur* x86 avec extension de virtualisation.

  Par exemple, les laboratoires de tests de performance d'ASA virtuel utilisent au minimum les éléments suivants : Cisco Unified Computing System (Cisco UCS®), serveur série C M4 avec les processeurs Intel Xeon® E5-2690v4 fonctionnant à 2,6 GHz.

vNIC recommandées

Les vNIC suivantes sont recommandées pour des performances optimales.

- i40e en mode Transmission directe PCI : dédié à la carte réseau physique du serveur à la machine virtuelle et transfère les données de paquets entre la carte réseau et la machine virtuelle par DMA (accès direct à la mémoire). Aucun cycle de CPU n'est nécessaire pour le déplacement des paquets.
- i40evf/ixgbe-vf : en fait, la même chose que ci-dessus (paquets DMA entre la carte réseau et la VM), mais permet de partager la carte réseau sur plusieurs VM. SR-IOV est généralement préféré, car il offre une plus grande souplesse de déploiement. Voir
- virtio : il s'agit d'un pilote de réseau para-virtualisé qui prend en charge le fonctionnement à 10 Gbit/s, mais nécessite également des cycles du CPU.

Remarque L'instance d'ASA virtuel s'exécutant sur le système KVM peut rencontrer des problèmes de connectivité des données avec l'interface SR-IOV en utilisant la version 2.17.4 du pilote vNIC i40e. Nous vous recommandons de mettre à niveau cette version de vNIC vers d'autres versions comme solution de contournement pour résoudre ce problème.

Optimisation des performances

Pour obtenir les meilleures performances avec ASA virtuel, vous pouvez apporter des ajustements à la machine virtuelle et à l'hôte. Consultez Réglage de la performance, à la page 59 pour de plus amples renseignements.

- **NUMA** : vous pouvez améliorer les performances d'ASA virtuel en isolant les ressources du CPU de la machine virtuelle invitée en un seul nœud d'accès à la mémoire non uniforme (NUMA). Consultez Lignes directrices NUMA, à la page 61 pour de plus amples renseignements.
- **Receive Side Scaling** (Dimensionnement côté réception) : l'ASA virtuel prend en charge Receive Côté Scaling (RSS), qui est une technologie utilisée par les adaptateurs réseau pour distribuer le trafic de réception réseau entre plusieurs cœurs de processeur. Consultez Files d'attente RX multiples pour le dimensionnement de la réception (RSS)., à la page 63 pour de plus amples renseignements.
- **VPN Optimization** (Optimisation du VPN) : consultez Optimisation du réseau privé virtuel (VPN), à la page 66 pour obtenir des considérations supplémentaires afin d'optimiser les performances du VPN avec l'ASA virtuel.

Mise en grappes

À partir de la version 9.17, la mise en grappe est prise en charge sur les instances d'ASA virtuel déployées sur KVM. Consultez la section Grappe ASA pour l'ASAv pour de plus amples renseignements.

Épinglage de CPU

L'épinglage de CPU est nécessaire pour que l'ASA virtuel fonctionne dans un environnement KVM; voir Activer l'épinglage du processeur (CPU), à la page 60.

Lignes directrices relatives au basculement pour la haute disponibilité

Pour les déploiements de basculement, assurez-vous que l'unité de secours a les mêmes droits de licence; par exemple, les deux unités doivent avoir le droit de 2 Gbit/s.

Important Lors de la création d'une paire à haute accessibilité à l'aide d'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.

ASA virtuel sur Proxmox VE

Proxmox Virtual Environment (VE) est une plateforme de virtualisation de serveurs à code source libre qui peut gérer les machines virtuelles KVM. Proxmox VE fournit également une interface de gestion web.

Lorsque vous déployez l'ASA virtuel sur Proxmox VE, vous devez configurer la VM pour qu'elle ait un port série émulé. Sans le port série, l'ASA virtuel entrera en boucle pendant le processus de démarrage. Toutes les tâches de gestion peuvent être effectuées à l'aide de l'interface de gestion web Proxmox VE.

Remarque Pour les utilisateurs avancés qui sont habitués au confort de l'interface Shell Unix ou de Windows Powershell, Proxmox VE fournit une interface de ligne de commande pour gérer tous les composants de votre environnement virtuel. Cette interface de ligne de commande dispose d'une fonction intelligente de complétion par tabulation et d'une documentation complète sous forme de pages de manuel UNIX.

Pour que l'ASA virtuel démarre correctement, la VM doit avoir un périphérique série configuré :

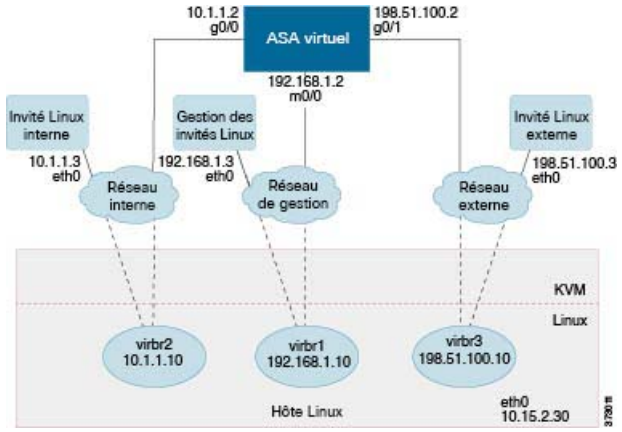
1. Dans le centre de gestion principal, sélectionnez la machine ASA virtuel dans l'arborescence de navigation de gauche.
2. Mettez la machine virtuelle hors tension.
3. Choisissez **Hardware (Matériel)** > **Add (Ajouter)** > **Network Device (Appareil réseau)** et ajoutez un port série.
4. Mettez l'ordinateur virtuel sous tension.
5. Accédez à la machine ASA virtuel à l'aide de Xterm.js.

Consultez la page Terminal série de Proxmox pour en savoir plus sur la configuration et l'activation du terminal sur l'invité ou le serveur.

Aperçu

La figure suivante montre un exemple de topologie de réseau avec ASA virtuel et KVM. Les procédures décrites dans ce chapitre reposent sur l'exemple de topologie. L'ASA virtuel agit comme pare-feu entre les réseaux interne et externe. Un réseau de gestion distinct est également configuré.

Illustration 6 : Exemple de déploiement d'ASA virtuel à l'aide de KVM



Prérequis

- Téléchargez le fichier qcow2 ASA virtuel à partir de Cisco.com et placez-le sur votre hôte Linux :

  http://www.cisco.com/go/asa-software

Remarque Une connexion à Cisco.com et un contrat de service Cisco sont requis.

- Aux fins de l'exemple de déploiement présenté dans ce document, nous supposons que vous utilisez Ubuntu 18.04 LTS. Installez les paquets suivants sur l'hôte Ubuntu 18.04 LTS :
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- Les performances sont affectées par l'hôte et sa configuration. Vous pouvez maximiser le débit de l'ASA virtuel sur KVM en réglant votre hôte. Pour les concepts génériques de réglage d'hôte, consultez NFV fournit des performances de traitement des paquets avec Intel.

- Voici des optimisations utiles pour Ubuntu 18.04 :
  - macvtap : pont Linux à haute performance; vous pouvez utiliser macvtap au lieu d'un pont Linux. Notez que vous devez configurer des paramètres précis pour utiliser macvtap au lieu du pont Linux.
  - Transparent Huge Pages : augmente la taille des pages de mémoire et est activé par défaut dans Ubuntu 18.04.

    Hyperthread désactivé : réduit deux vCPU en un seul cœur.
  - txqueuelength : augmente la longueur de la file d'attente par défaut à 4 000 paquets et réduit le taux d'abandon.
  - épinglage : applique des processus qemu et vhost à des cœurs de CPU spécifiques; dans certaines conditions, l'épinglage augmente considérablement les performances.
- Pour en savoir plus sur l'optimisation d'une distribution basée sur RHEL, consultez le Guide de réglage et d'optimisation de la virtualisation Red Hat Enterprise Linux 7.
- Pour la compatibilité du logiciel ASA et des hyperviseurs ASA virtuel, consultez la section Compatibilité Cisco Cisco Secure Firewall ASA.

Préparer le fichier de configuration Day0 (Jour0)

Vous pouvez préparer un fichier de configuration Day0 (Jour0) avant de lancer l'ASA virtuel. Ce fichier est un fichier texte qui contient la configuration ASA virtuel appliquée lors du lancement de l'ASA virtuel. Cette configuration initiale est placée dans un fichier texte nommé « day0-config » dans un répertoire de travail que vous avez choisi, puis manipulée dans un fichier day0.iso qui est monté et lu lors du premier démarrage. Au minimum, le fichier de configuration Day0 (Jour0) doit contenir des commandes pour activer l'interface de gestion et configurer le serveur SSH pour l'authentification par clé publique, mais il peut également contenir une configuration ASA complète.

Le fichier day0.iso (votre fichier day0.iso personnalisé ou le fichier day0.iso par défaut) doit être disponible lors du premier démarrage :

- Pour autoriser automatiquement l'ASA virtuel lors du déploiement initial, placez le jeton d'identité de licence Smart (ID) que vous avez téléchargé à partir de Cisco Smart Software Manager dans un fichier texte nommé « idtoken » dans le même répertoire que le fichier de configuration Day0 (Jour0).
- Si vous souhaitez accéder à l'ASA virtuel à partir du **port série** de l'hyperviseur au lieu de la console virtuelle VGA, vous devez inclure le paramètre série de la console dans le fichier de configuration Day0 (Jour0) pour utiliser le port série lors du premier démarrage.
- Si vous souhaitez déployer l'ASA virtuel en mode transparent, vous devez utiliser un fichier de configuration ASA connu en cours d'exécution en mode transparent comme fichier de configuration Day0 (Jour0). Cela ne s'applique pas à un fichier de configuration Day0 (Jour0) pour un pare-feu routé.

Remarque Nous utilisons Linux dans cet exemple, mais il existe des utilitaires similaires pour Windows.

Procédure

Étape 1 Saisissez la configuration de l'interface de ligne de commande pour l'ASA virtuel dans un fichier texte appelé « day0-config ». Ajoutez des configurations d'interface pour les trois interfaces et toute autre configuration de votre choix.

La première ligne doit commencer par la version de l'ASA. La configuration day0-config doit être une configuration ASA valide. La meilleure façon de générer la configuration day0 (jour0) est de copier les parties pertinentes d'une configuration en cours d'exécution à partir d'un ASA ou d'un ASA virtuel existant. L'ordre des lignes dans la configuration day0 (jour0) est important et doit correspondre à l'ordre observé dans une sortie de commande **show running-config** existante.

Exemple :

```
ASA Version 9.4.1
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
```

Étape 2 (Facultatif) Pour l'octroi de licences automatisé lors du déploiement initial d'ASA virtuel, assurez-vous que les renseignements suivants se trouvent dans le fichier day0-config :

- Adresse IP de l'interface de gestion
- (Facultatif) Mandataire HTTP à utiliser pour les licences Smart
- Une commande de **route** qui active la connectivité au mandataire HTTP (si précisé) ou à tools.cisco.com
- Un serveur DNS qui corrige tools.cisco.com en adresse IP
- La configuration de licence Smart précise la licence ASA virtuel que vous demandez
- (Facultatif) Un nom de domaine unique pour que l'ASA virtuel soit plus facile à trouver dans CSSM

Étape 3 (Facultatif) Téléchargez le fichier de jeton d'identité de la licence Smart émis par Cisco Smart Software Manager sur votre ordinateur, copiez le jeton d'ID à partir du fichier téléchargé et placez-le dans un fichier texte nommé « idtoken » qui contient uniquement le jeton d'ID.

Étape 4 Générez le CD-ROM virtuel en convertissant le fichier texte en fichier ISO :

Exemple :

```
stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size (bytes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

Le jeton d'identité enregistre automatiquement l'ASA virtuel sur le serveur de licences Smart.

Étape 5 Répétez les étapes 1 à 5 pour créer des fichiers de configuration par défaut distincts avec les adresses IP appropriées pour chaque ASA virtuel que vous souhaitez déployer.

Préparer les fichiers XML de pont virtuel

Vous devez configurer des réseaux virtuels qui connectent les invités ASA virtuel à l'hôte KVM et qui connectent les invités entre eux.

Remarque Cette procédure n'établit pas la connectivité au monde externe en dehors de l'hôte KVM.

Préparez les fichiers XML de pont virtuel sur l'hôte KVM. Pour l'exemple de topologie de réseau virtuel décrit dans Préparer le fichier de configuration Day0 (Jour0), à la page 55, vous avez besoin des trois fichiers de pont virtuel suivants : virbr1.xml, virbr2.xml et virbr3.xml (vous devez utiliser ces trois noms de fichiers; par exemple, virbr0 n'est pas autorisé, car il existe déjà). Chaque fichier contient les renseignements nécessaires pour configurer les ponts virtuels. Vous devez attribuer au pont virtuel un nom et une adresse MAC uniques. L'attribution d'une adresse IP est facultative.

Procédure

Étape 1 Créez trois fichiers XML de pont de réseau virtuel. Par exemple, virbr1.xml, virbr2.xml et virbr3.xml :

Exemple :

```
<network>
<name>virbr1</name>
<bridge name='virbr1' stp='on' delay='0' />
<mac address='52:54:00:05:6e:00' />
<ip address='192.168.1.10' netmask='255.255.255.0' />
</network>
```

Exemple :

```
<network>
<name>virbr2</name>
```

```
<bridge name='virbr2' stp='on' delay='0' />
<mac address='52:54:00:05:6e:01' />
<ip address='10.1.1.10' netmask='255.255.255.0' />
</network>
```

Exemple :

```
<network>
<name>virbr3</name>
<bridge name='virbr3' stp='on' delay='0' />
<mac address='52:54:00:05:6e:02' />
<ip address='198.51.100.10' netmask='255.255.255.0' />
</network>
```

Étape 2 Créez un script qui contient les éléments suivants (dans notre exemple, nous nommons le script virt_network_setup.sh) :

```
virsh net-create virbr1.xml
virsh net-create virbr2.xml
virsh net-create virbr3.xml
```

Étape 3 Exécutez ce script pour configurer le réseau virtuel. Le script affiche les réseaux virtuels. Les réseaux restent opérationnels tant que l'hôte KVM est en cours d'exécution.

```
stack@user-ubuntu:-/KvmAsa$ virt_network_setup.sh
```

Remarque
Si vous rechargez l'hôte Linux, vous devez réexécuter le script virt_network_setup.sh. Il ne persiste pas pendant les redémarrages.

Étape 4 Vérifiez que les réseaux virtuels ont été créés :

```
stack@user-ubuntu:-/KvmAsa$ brctl show
bridge name bridge id STP enabled Interfaces
virbr0 8000.0000000000000 yes
virbr1 8000.5254000056eed yes virb1-nic
virbr2 8000.5254000056eee yes virb2-nic
virbr3 8000.5254000056eec yes virb3-nic
stack@user-ubuntu:-/KvmAsa$
```

Étape 5 Affichez l'adresse IP attribuée au pont virbr1. Voici l'adresse IP que vous avez attribuée dans le fichier XML.

```
stack@user-ubuntu:-/KvmAsa$ ip address show virbr1
S: virbr1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
link/ether 52:54:00:05:6e:00 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.10/24 brd 192.168.1.255 scope global virbr1
valid_lft forever preferred_lft forever
```

Déployer l'ASA virtuel

Utilisez un script de déploiement basé sur virt-install pour lancer l'ASA virtuel.

Procédure

Étape 1 Créez un script virt-install appelé « virt_install_asav.sh ».

Le nom de la machine ASA virtuel doit être unique pour toutes les autres VM sur cet hôte KVM.

L'ASA virtuel prend en charge jusqu'à 10 réseaux. Cet exemple utilise trois réseaux. L'ordre des clauses de pont de réseau est important. La première répertoriée est toujours l'interface de gestion de l'ASA virtuel (Management 0/0), la deuxième répertoriée est GigabitEthernet 0/0 de l'ASA virtuel et la troisième répertoriée est GigabitEthernet 0/1 de l'ASA virtuel et ainsi de suite jusqu'à GigabitEthernet 0/8. La carte réseau virtuelle doit être Virtio.

Exemple :

```
virt-install \
--connect=qemu:///system \
--network network=default,model=virtio \
--network network=default,model=virtio \
--network network=default,model=virtio \
--name=asav \
--cpu host \
--arch=x86_64 \
--machine=pc-1.0 \
--vcpus=1 \
--ram=2048 \
--os-type=linux \
--virt-type=kvm \
--import \
--disk path=/home/kvmperf/Images/desmo.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
--disk path=/home/kvmperf/asav_day0.iso,format=iso,device=cdrom \
--console pty,target_type=virtio \
--serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet
```

Étape 2 Exécutez le script virt_install :

Exemple :

```
stack@user-ubuntu:-/KvmAsa$ ./virt_install_asav.sh

Starting install...
Creating domain...
```

Une fenêtre apparaît, affichant la console de la VM. Vous pouvez voir que la VM démarre. Le démarrage de la VM prend quelques minutes. Une fois que la VM arrête de démarrer, vous pouvez exécuter des commandes de l'interface de ligne de commande à partir de l'écran de la console.

Réglage de la performance

Amélioration des performances pour les configurations KVM

Vous pouvez augmenter les performances d'un ASA virtuel dans l'environnement KVM en modifiant les paramètres sur l'hôte KVM. Ces paramètres sont indépendants des paramètres de configuration du serveur hôte. Cette option est disponible dans Red Hat Enterprise Linux 7.0 KVM.

Vous pouvez améliorer les performances des configurations KVM en activant l'épinglage CPU.

Activer l'épinglage du processeur (CPU)

ASA virtuel exige que vous utilisiez l'option d'affinité CPU KVM pour améliorer la performance de l'ASA virtuel dans les environnements KVM. L'affinité du processeur, ou l'épinglage CPU, permet de lier et de dissocier un processus ou un fil à une unité de traitement centrale (CPU) ou à une plage de CPU, de sorte que le processus ou le fil ne s'exécutera que sur l'unité ou les unités de traitement centrale (CPU) désignées plutôt que sur n'importe quelle CPU.

Configurez les associations d'hôtes pour déployer les instances qui utilisent l'épinglage CPU sur différents hôtes des instances qui ne le font pas, afin d'éviter que les instances non épinglées utilisent les exigences en matière de ressource des instances épinglées.

Attention Ne déployez pas des instances avec la topologie NIMA sur les mêmes hôtes que les instances qui n'ont pas la topologie NIMA.

Pour utiliser cette option, configurez l'épinglage CPU sur l'hôte KVM.

Procédure

Étape 1 Dans l'environnement d'hôte KVM, vérifiez la topologie de l'hôte pour trouver le nombre de vCPU disponibles pour l'épinglage :

Exemple :

```
virsh nodeinfo
```

Étape 2 Vérifiez les numéros de vCPU disponibles :

Exemple :

```
virsh capabilities
```

Étape 3 Épinglez les vCPU aux ensembles de cœurs de processeur :

Exemple :

```
virsh vcpupin <vm-name> <vcpu-number> <host-core-number>
```

La commande **virsh vcupinin** doit être exécutée pour chaque vCPU sur votre ASA virtuel. L'exemple suivant montre les commandes KVM nécessaires si vous avez une configuration ASA virtuel avec quatre vCPU et que l'hôte a huit cœurs :

```
virsh vcpupin asav 0 2
virsh vcpupin asav 1 3
virsh vcpupin asav 2 4
virsh vcpupin asav 3 5
```

Le nombre de cœurs de l'hôte peut être n'importe quel nombre entre 0 et 7. Pour plus d'informations, consultez la documentation KVM.

Remarque
Lors de la configuration de l'épinglage CPU, tenez compte de la topologie CPU du serveur hôte. Si vous utilisez un serveur configuré avec plusieurs cœurs, ne configurez pas l'épinglage CPU sur plusieurs connecteurs.

L'inconvénient de l'amélioration des performances de la configuration KVM est qu'elle nécessite des ressources système dédiées.

Lignes directrices NUMA

L'accès mémoire non uniforme (NUMA, Non-Uniform Memory Access) est une architecture de mémoire partagée qui décrit le placement des modules de mémoire principaux en ce qui concerne les processeurs dans un système multiprocesseur. Lorsqu'un processeur accède à la mémoire qui ne se trouve pas dans son propre nœud (mémoire distante), les données doivent être transférées sur la connexion NUMA à un débit plus lent qu'il ne le serait lors de l'accès à la mémoire locale.

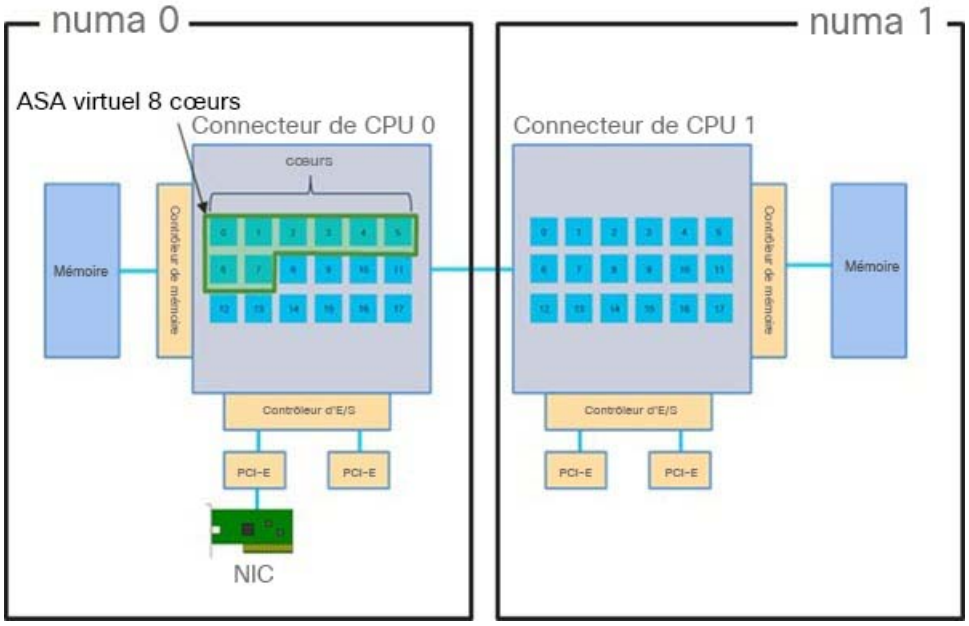
L'architecture du serveur x86 est composée de plusieurs connecteurs et de plusieurs cœurs dans un connecteur. Chaque connecteur CPU, ainsi que sa mémoire et son entrée-sortie, est appelé nœud NUMA. Pour lire efficacement les paquets à partir de la mémoire, les applications invitées et les périphériques associés (comme la carte d'interface réseau) doivent résider sur le même nœud.

Pour une performance ASA virtuel optimale :

- La machine ASA virtuel doit fonctionner sur un seul nœud numa. Si un seul ASA virtuel est déployé de sorte qu'il fonctionne sur deux connecteurs, la performance sera considérablement réduite.
- Un ASA virtuel à 8 cœurs (Illustration 7 : Exemple d'architecture NUMA ASA virtuel à 8 cœurs , à la page 62) exige que chaque connecteur du CPU hôte ait au moins 8 cœurs par connecteur. Il faut tenir compte des autres machines virtuelles en cours d'exécution sur le serveur.
- Un ASA virtuel à 16 cœurs (Illustration 8 : Exemple d'architecture NUMA ASA virtuel à 16 cœurs, à la page 62) exige que chaque connecteur du CPU hôte ait un minimum de 16 cœurs par connecteur. Il faut tenir compte des autres machines virtuelles en cours d'exécution sur le serveur.
- La carte réseau (NIC) doit se trouver sur le même nœud NUMA que la machine ASA virtuel.

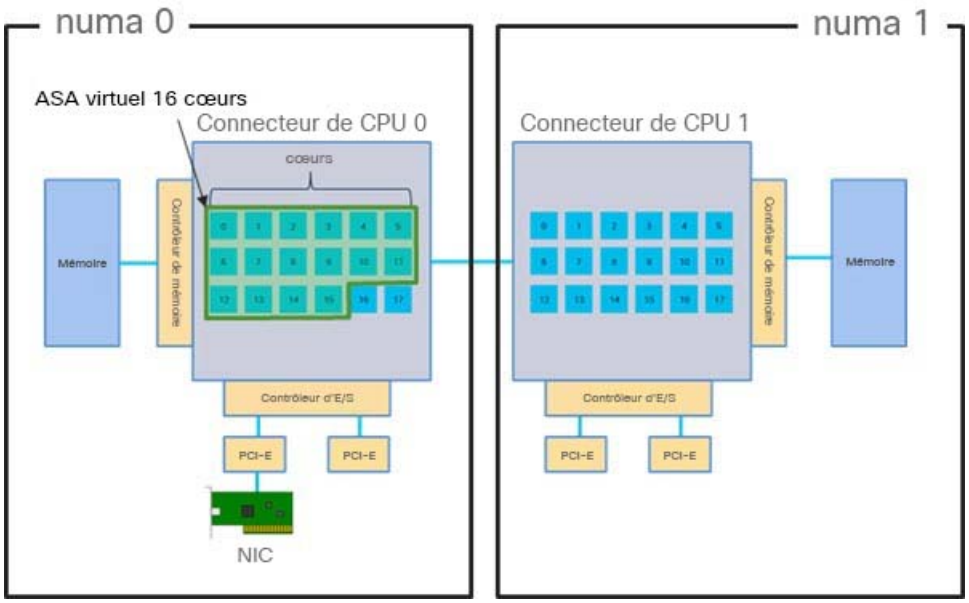
La figure suivante montre un serveur avec deux connecteurs pour CPU, chaque CPU ayant 18 cœurs. L'ASA virtuel à 8 cœurs exige que chaque connecteur du CPU hôte ait au moins 8 cœurs.

Illustration 7 : Exemple d'architecture NUMA ASA virtuel à 8 cœurs



La figure suivante montre un serveur avec deux connecteurs pour CPU, chaque CPU ayant 18 cœurs. L'ASA virtuel à 16 cœurs exige que chaque connecteur du CPU hôte ait au moins 16 cœurs.

Illustration 8 : Exemple d'architecture NUMA ASA virtuel à 16 cœurs



Optimisation NUMA

Idéalement, la machine ASA virtuel devrait fonctionner sur le même nœud numa que celui des cartes réseau (NIC). Voici la marche à suivre :

1. Déterminez sur quel nœud se trouvent les cartes réseau en utilisant « lstopo » pour afficher un diagramme des nœuds. Localisez les cartes réseau et notez le nœud auquel elles sont connectées.
2. Sur l'hôte KVM, utilisez `virsh list` pour trouver l'ASA virtuel.
3. Modifier la machine virtuelle en utilisant : `virsh edit <Numéro de machine virtuelle>`.
4. Alignez ASA virtuel sur le nœud choisi. Les exemples suivants supposent des nœuds à 18 cœurs.

   Aligner sur le nœud 0 :

   ```
   <vcpu placement='static' cpuset='0-17'>16</vcpu>
   <numatune>
       <memory mode='strict' nodeset='0'/>
   </numatune>
   ```

   Aligner sur le nœud 1 :

   ```
   <vcpu placement='static' cpuset='18-35'>16</vcpu>
   <numatune>
       <memory mode='strict' nodeset='1'/>
   </numatune>
   ```

5. Enregistrez la modification de .xml et redémarrez la machine ASA virtuel.
6. Pour vous assurer que votre machine virtuelle fonctionne sur le nœud souhaité, effectuez un `ps aux | grep <nom de votre machine virtuelle ASAv>` pour obtenir l'ID de processus.
7. Exécutez `sudo numastat -c <ID de processus de la machine virtuelle ASAv>` pour voir si la machine ASA virtuel est correctement alignée.

Vous trouverez plus d'informations sur l'utilisation de la mise au point de NUMA avec KVM dans le document RedHat 9.3. libvirt NUMA Tuning.

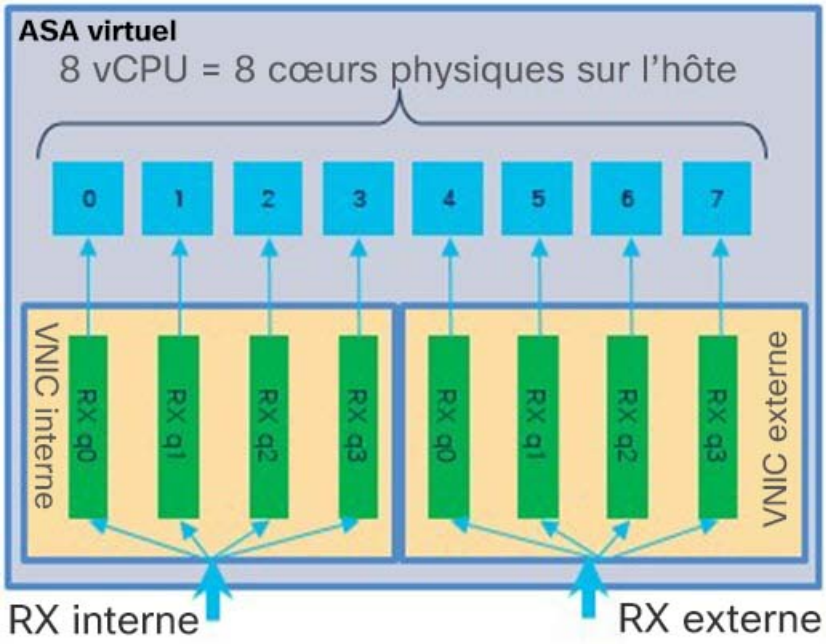
Files d'attente RX multiples pour le dimensionnement de la réception (RSS).

L'ASA virtuel prend en charge le dimensionnement de la réception (RSS), qui est une technologie utilisée par les adaptateurs réseau pour distribuer le trafic de réception réseau entre plusieurs cœurs de processeur. Pour un débit maximal, chaque vCPU (cœur) doit avoir sa propre file d'attente RX NIC. Notez qu'un déploiement typique de réseau privé virtuel (VPN) d'accès à distance peut utiliser une seule paire d'interfaces interne/externe.

Important La version 9.13(1) ou ultérieure d'ASA virtuel est nécessaire pour utiliser plusieurs files d'attente RX. Pour KVM, la version *libvirt* doit être au moins 1.0.6.

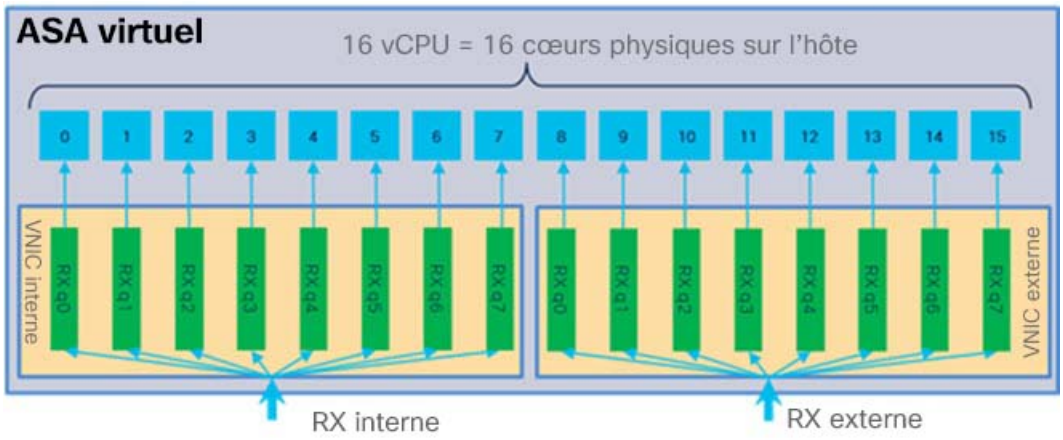
Pour une machine virtuelle à 8 cœurs avec une paire d'interfaces interne/externe, chaque interface aura 4 files d'attente RX, comme indiqué dans Illustration 9 : Files d'attente RX RSS à 8 cœurs ASA virtuel , à la page 64.

Illustration 9 : Files d'attente RX RSS à 8 cœurs ASA virtuel



Pour une machine virtuelle à 16 cœurs avec une paire d'interfaces interne/externe, chaque interface aura 8 files d'attente RX, comme indiqué dans Illustration 10 : Files d'attente RX RSS à 16 cœurs ASA virtuel, à la page 64.

Illustration 10 : Files d'attente RX RSS à 16 cœurs ASA virtuel



Le tableau suivant présente les vNIC de l'ASA virtuelpour KVM et le nombre de files d'attente RX prises en charge. Consultez vNIC recommandées, à la page 52 pour obtenir des descriptions des vNIC prises en charge.

Tableau 12 : NIC/vNIC recommandées par KVM

Carte NIC	Pilote vNIC	Technologie de pilote	Nombre de files d'attente RX	Rendement
x710	i40e	PCI Passthrough (transmission directe de PCI)	8 maximum	Les modes PCI Passthrough et SR-IOV pour le x710 offrent les meilleures performances. SR-IOV est généralement préféré pour les déploiements virtuels, car la carte d'interface réseau (NIC) peut être partagée sur plusieurs machines virtuelles.
	i40evf	SR-IOV	8	
x520	ixgbe	PCI Passthrough (transmission directe de PCI)	6	La carte réseau x520 affiche des performances de 10 à 30 % inférieures à celles de la x710. Les modes PCI Passthrough et SR-IOV pour le x520 offrent des performances similaires. SR-IOV est généralement préféré pour les déploiements virtuels, car la carte d'interface réseau (NIC) peut être partagée sur plusieurs machines virtuelles.
	ixgbe-vf	SR-IOV	2	
S. O.	virtio	Paravirtualisation	8 maximum	Non recommandé pour ASAv100. Pour d'autres déploiements, consultez Activer la prise en charge multifile d'attente pour Virtio sur KVM, à la page 65.

Activer la prise en charge multifile d'attente pour Virtio sur KVM

L'exemple suivant montre comment configurer le nombre de files d'attente RX de la carte réseau Virtio à 4 à l'aide de virsh pour modifier le xml de libvirt :

```
<interface type='bridge'>
 <mac address='52:54:00:43:6e:3f'/>
 <source bridge='clients'/>
 <model type='virtio'/>
 <driver name='vhost' queues='4'/>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
</interface>
```

Important La version *libvirt* doit être au moins 1.0.6 pour prendre en charge plusieurs files d'attente RX.

Optimisation du réseau privé virtuel (VPN)

Voici quelques considérations supplémentaires pour optimiser les performances du VPN avec l'ASA virtuel.

- IPSec a un débit plus élevé que DTLS.
- Chiffrement : GCM a environ deux fois le débit de CBC.

Provisionnement d'interface SR-IOV

SR-IOV permet à plusieurs machines virtuelles de partager un seul adaptateur réseau PCIe à l'intérieur d'un hôte. SR-IOV définit ces fonctions :

- Fonction physique (PF) : les PF sont des fonctions PCIe complètes qui comprennent les capacités SR-IOV. Celles-ci s'affichent comme des cartes réseau (NIC) statiques normales sur le serveur hôte.
- Fonction virtuelle (VF) : les VF sont des fonctions PCIe allégées qui aident au transfert de données. Une VF est dérivée d'une PF et gérée par l'intermédiaire d'une PF.

Les VF peuvent fournir une connectivité allant jusqu'à 10 Gbit/s à la machine ASA virtuel dans une structure de système d'exploitation virtualisé. Cette section explique comment configurer les VF dans un environnement KVM. La prise en charge de SR-IOV sur l'ASA virtuel est expliquée dans ASA virtuel et provisionnement de l'interface SR-IOV, à la page 12.

Sur ASAv5 et ASAv10, le pilote VMXNET3 est fortement recommandé pour une performance optimale. De plus, l'interface SR-IOV, lorsqu'elle est utilisée en combinaison (mélange d'interfaces), améliore la performance du réseau avec ASA virtuel, en particulier avec l'allocation de plus de cœurs et de ressources pour le processeur (CPU).

Exigences pour le provisionnement de l'interface SR-IOV

Si vous avez une carte réseau physique qui prend en charge SR-IOV, vous pouvez associer des VF compatibles avec SR-IOV ou des cartes réseau virtuelles (vNIC) à l'instance ASA virtuel. SR-IOV nécessite également une prise en charge dans le BIOS ainsi que dans l'instance de système d'exploitation ou l'hyperviseur qui s'exécute sur le matériel. Vous trouverez ci-dessous une liste de lignes directrices générales pour le provisionnement de l'interface SR-IOV pour l'exécution d'ASA virtuel dans un environnement KVM :

- Vous avez besoin d'une carte d'interface réseau physique compatible avec SR-IOV dans le serveur hôte; voir Lignes directrices et limites des interfaces SR-IOV, à la page 13.
- Vous devez activer la virtualisation dans le BIOS sur votre serveur d'hôte. Consultez la documentation de votre prestataire pour en savoir plus.
- Vous avez besoin d'activer la prise en charge globale d'IAMMU pour SR-IOV dans le BIOS sur votre serveur d'hôte. Consultez la documentation de votre prestataire de matériel pour en savoir plus.
- L'ASA virtuel sur KVM à l'aide de l'interface SR-IOV prend en charge le mélange de types d'interfaces. Vous pouvez utiliser SR-IOV ou VMXNET3 pour l'interface de gestion et SR-IOV pour l'interface de données.

Modifier le BIOS et le système d'exploitation de l'hôte KVM

Cette section montre diverses étapes d'installation et de configuration pour le provisionnement des interfaces SR-IOV sur un système KVM. Les renseignements figurant dans cette section ont été créés à partir de

périphériques dans un environnement de laboratoire spécifique, en utilisant Ubuntu 14.04 sur un serveur Cisco série UCS C avec un adaptateur de serveur Ethernet Intel X520 - DA2.

Avant de commencer

- Assurez-vous d'avoir une carte d'interface de réseau (NIC) compatible avec SR-IOV.
- Assurez-vous que les fonctionnalités des technologies de virtualisation Intel (VT-x) et VT-d sont activées.

Remarque Certains fabricants de systèmes désactivent ces extensions par défaut. Nous vous recommandons de vérifier le processus avec la documentation du fournisseur, car différents systèmes ont des méthodes différentes pour accéder aux paramètres BIOS et les modifier.

- Assurez-vous que tous les modules, toutes les bibliothèques, tous les outils utilisateur et toutes les utilitaires Linux ont été installés lors de l'installation du système d'exploitation; voir Prérequis, à la page 54.
- Assurez-vous que l'interface physique est à l'état UP. Vérifiez avec ifconfig <*ethname*>.

Procédure

Étape 1 Connectez-vous à votre système à l'aide du compte utilisateur et du mot de passe « root » (racine).

Étape 2 Vérifiez que Intel VT-d est activé.

Exemple :

```
kvmuser@kvm-host:/$ dmesg | grep -e DMAR -e IOMMU
[    0.000000] ACPI: DMAR 0x000000006F9A4C68 000140 (v01 Cisco0 CiscoUCS 00000001 INTL 20091013)
[    0.000000] DMAR: IOMMU enabled
```

La dernière ligne indique que VT-d est activé.

Étape 3 Activez Intel VT-d dans le noyau en ajoutant le paramètre *intel_iommu=on* à l'entrée GRUB_CMDLINE_LINUX dans le fichier de configuration */etc/default/grub*.

Exemple :

```
# vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... intel_iommu=on"
...
```

Remarque
Si vous utilisez un processeur AMD, ajoutez plutôt *amd_iommu=on* aux paramètres de démarrage.

Étape 4 Redémarrez le serveur pour que la modification iommu prenne effet.

Exemple :

```
> shutdown -r now
```

Étape 5 Créez des VF en écrivant une valeur appropriée au paramètre *sriov_numvfs* via l'interface *sysfs* en utilisant le format suivant :

```
#echo n > /sys/class/net/device name/device/sriov_numvfs
```

Pour vous assurer que le nombre souhaité de VF est créé à chaque cycle d'alimentation du serveur, vous devez ajouter la commande ci-dessus au fichier *rc.local*, qui se trouve dans le répertoire */etc/rc.d/*. Le système d'exploitation Linux exécute le script *rc.local* à la fin du processus de démarrage.

Par exemple, les éléments suivants montrent la création d'une VF par port. Les interfaces pour votre configuration particulière varient.

Exemple :

```
echo '1' > /sys/class/net/eth4/device/sriov_numvfs
echo '1' > /sys/class/net/eth5/device/sriov_numvfs
echo '1' > /sys/class/net/eth6/device/sriov_numvfs
echo '1' > /sys/class/net/eth7/device/sriov_numvfs
```

Étape 6 Redémarrez le serveur.

Exemple :

```
> shutdown -r now
```

Étape 7 Vérifiez que les VF ont été créées à l'aide de *lspci*.

Exemple :

```
 > lspci | grep -i "Virtual Function"
kvmuser@kvm-racetrack:~$ lspci | grep -i "Virtual Function"
0a:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.1 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.2 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.3 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
```

Remarque
Vous verrez des interfaces supplémentaires à l'aide de la commande **ifconfig**.

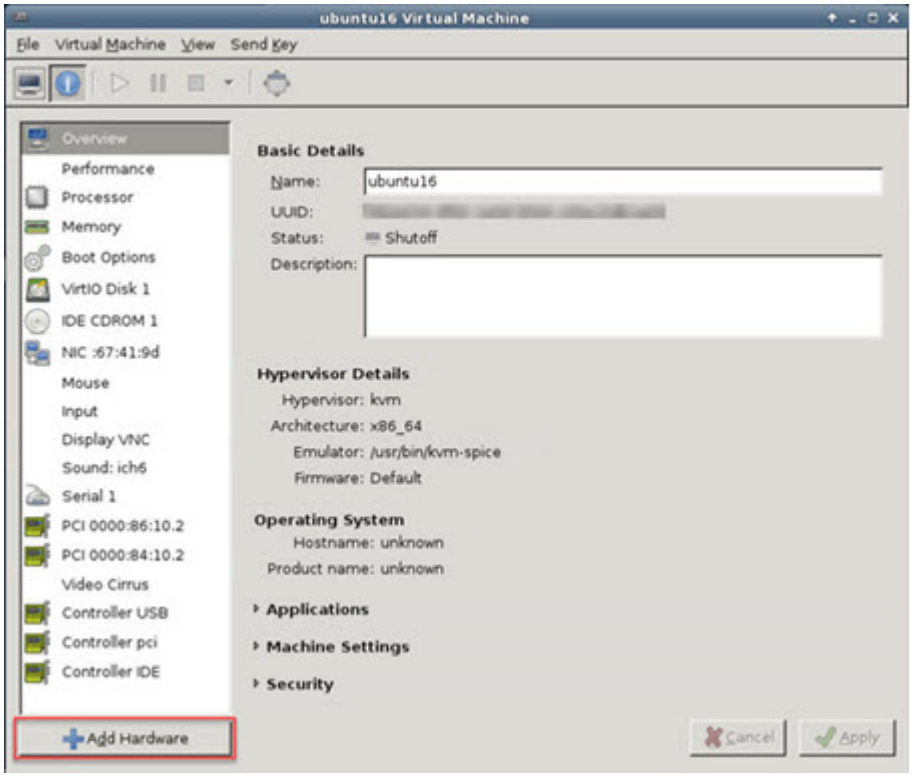
Affecter des périphériques PCI à l'ASA virtuel

Une fois que vous avez créé des VF, vous pouvez les ajouter à l'ASA virtuel comme vous ajouteriez n'importe quel périphérique PCI. L'exemple suivant explique comment ajouter un contrôleur VF Ethernet à un ASA virtuel à l'aide de l'outil graphique **virt-manager**.

Procédure

Étape 1 Ouvrez l'ASA virtuel et cliquez sur le bouton **Add Hardware** (Ajouter du matériel) pour ajouter un nouveau périphérique à la machine virtuelle.

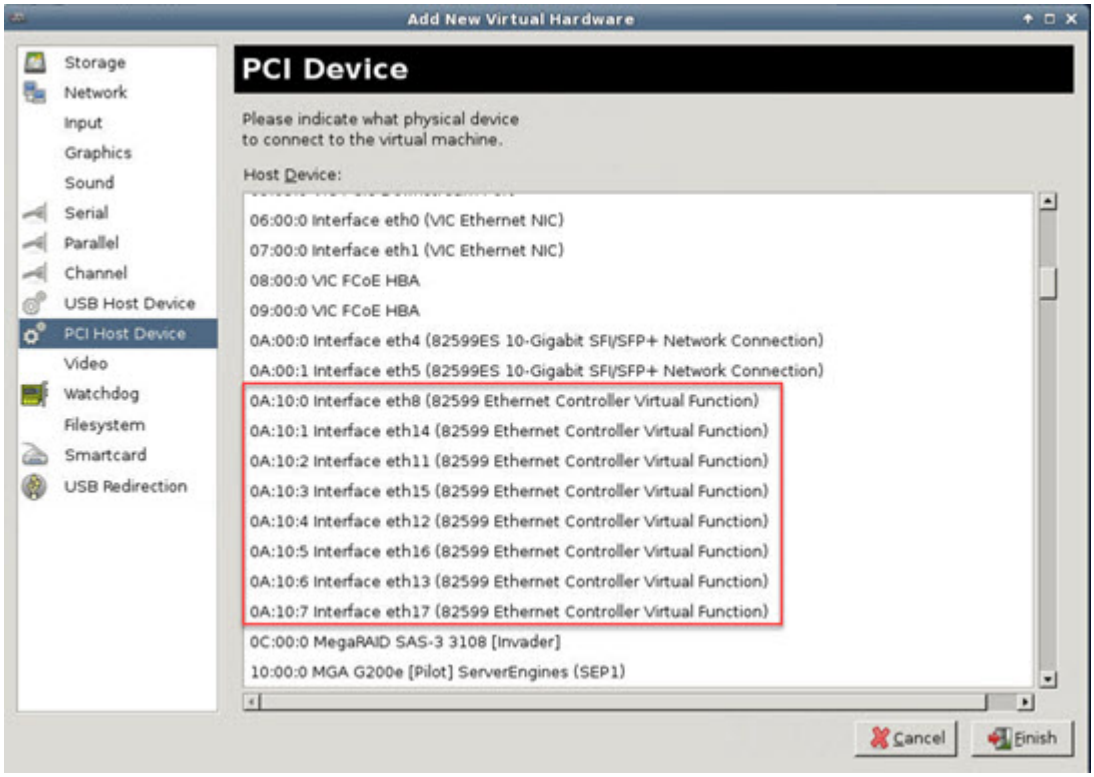
Illustration 11 : Ajouter du matériel



Étape 2 Cliquez sur **PCI Host Device** (Périphérique hôte PCI) dans la liste **Hardware** (Matériel) du volet gauche.

La liste des périphériques PCI, y compris les VF, apparaît dans le volet central.

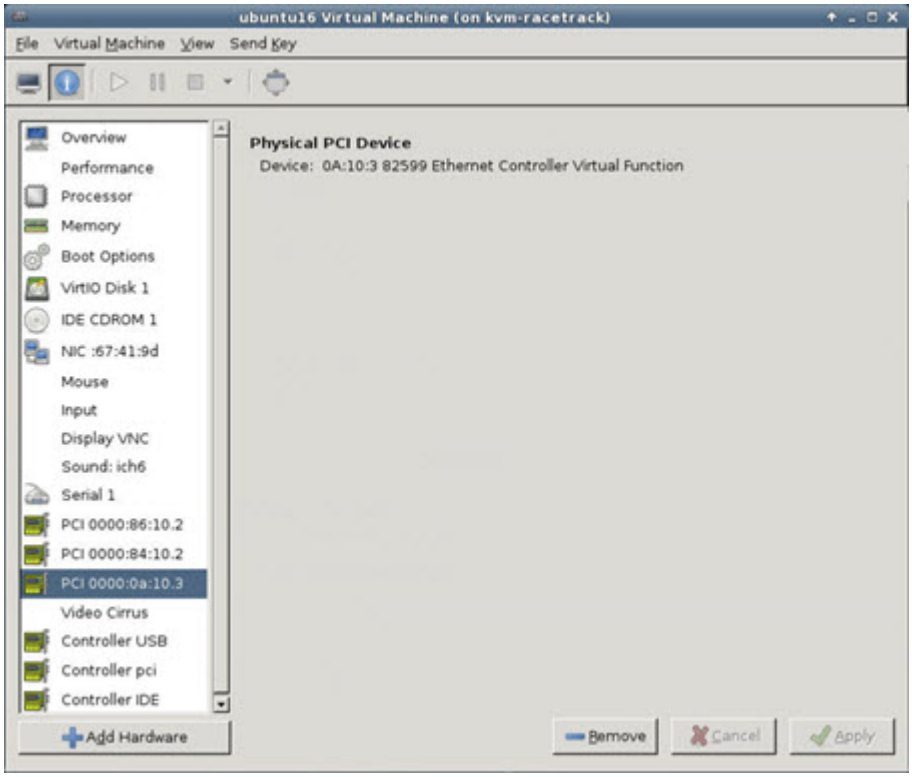
Illustration 12 : Liste des fonctions virtuelles



Étape 3 Sélectionnez l'une des fonctions virtuelles disponibles et cliquez sur **Finish** (Terminer).

Le périphérique PCI apparaît dans la liste du matériel; notez la description du périphérique comme fonction virtuelle de contrôleur Ethernet.

Illustration 13 : Fonction virtuelle ajoutée



Prochaine étape

- Utilisez la commande **show interface** (afficher l'interface) de la ligne de commande ASA virtuel pour vérifier les interfaces nouvellement configurées.
- Pour en savoir plus, utilisez le mode de configuration d'interface sur l'ASA virtuel pour configurer et activer l'interface pour la transmission et la réception du trafic; consultez le chapitre *Configuration de base de l'interface* du Guide de configuration de l'interface de ligne de commande pour les opérations générales de série Cisco Cisco Secure Firewall ASA.

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 sur environ 30 à 40 % de la capacité totale du processeur en dehors des heures de pointe et sur environ 60 à 70 % de capacité pendant les heures de pointe.

Important À partir de la version 9.13(1), n'importe quelle licence d'ASA virtuel peut être utilisée sur n'importe quelle configuration de vCPU/de mémoire d'ASA virtuel. Cela permet aux clients d'ASA virtuel d'exécuter une grande variété de profils de ressources VM.

Utilisation de vCPU dans ASA virtuel

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 vSphere comprend l'utilisation de l'ASA virtuel comme décrit plus :

- Délai d'inactivité d'ASA virtuel
- %SYS surdébit utilisé pour la machine virtuelle ASA
- Surdébit du déplacement des paquets entre les vSwitches, les vNIC et les pNIC. Ce surdébit peut être assez important.

Exemple d'utilisation du processeur

La commande **show cpu usage** (afficher l'utilisation du processeur) peut être utilisée pour afficher les statistiques d'utilisation du processeur.

Exemple

```
Ciscoasa#show cpu usage

Utilisation du processeur pendant 5 secondes = 1 %; 1 minute : 2 %; 5 minutes : 1 %
```

Voici un exemple dans lequel l'utilisation de vCPU signalée est sensiblement différente :

- Rapports ASA virtuel : 40 %
- DP : 35 %
- Processus externes : 5 %
- 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.

Rapport d'utilisation du processeur (CPU) de KVM

La

```
virsh cpu-stats domain --total start count
```

fournit les renseignements statistiques du CPU sur la machine virtuelle invitée indiquée. Par défaut, elle affiche les statistiques de tous les CPU, ainsi que le total. L'option `--total` n'affiche que les statistiques totales. L'option `--count` n'affiche que les statistiques du *nombre* de CPU.

Des outils comme OProfile, top, etc. donnent l'utilisation totale du processeur d'une VM KVM particulière, qui inclut l'utilisation du processeur de l'hyperviseur et de la VM. De même, des outils comme XenMon, qui sont propres à Xen VMM, attribuent une utilisation totale du CPU de l'hyperviseur Xen, c'est-à-dire du domaine 0, mais ne le séparent pas en fonction de l'utilisation de l'hyperviseur par VM.

À côté de cela, certains outils existent dans les cadres d'informatique en nuage comme OpenNebula, qui ne fournit que des renseignements approximatifs sur le pourcentage de CPU virtuel utilisé par une VM.

Graphiques ASA virtuel et KVM

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et KVM :

- Les numéros de graphique KVM sont toujours supérieurs aux numéros d'ASA virtuel.
- KVM l'appelle « %CPU usage »; l'ASA virtuel l'appelle « %CPU utilization ».

Les termes « %CPU utilization » et « %CPU usage » ont des significations différentes :

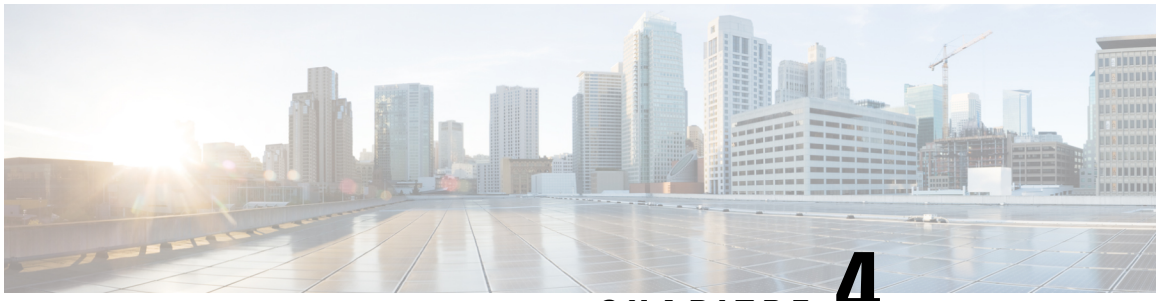
- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

KVM 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



CHAPITRE 4

Déployer l'ASA virtuel sur AWS en nuage

Vous pouvez déployer l'ASA virtuel sur le nuage Amazon Web Services (AWS).

Important À partir de la version 9.13(1), toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge. Cela permet aux ASA virtuel clients de fonctionner sur une grande variété de profils de ressources VM. Cela augmente également le nombre d'instances AWS prises en charge.

- Aperçu, à la page 75
- Prérequis, à la page 78
- Lignes directrices et limites relatives à la licence, à la page 78
- Migration de la configuration et authentification SSH, à la page 79
- Exemple de topologie de réseau, à la page 80
- Déploiement ASA virtuel, à la page 81
- Intégration du service Amazon GuardDuty et Défense contre les menaces virtuelles, à la page 84
- À propos de l'intégration d'Cisco Secure Firewall ASA virtuel et GuardDuty, à la page 84
- Plateformes logicielles prises en charge, à la page 87
- Lignes directrices et limites pour l'intégration d'Amazon GuardDuty et de Cisco Secure Firewall ASA Virtual, à la page 87
- Intégrer Amazon GuardDuty avec ASA virtuel, à la page 88
- Mettre à jour la configuration de déploiement de solution existante, à la page 100
- Réglage de la performance, à la page 101

Aperçu

L'ASA virtuel exécute le même logiciel que les ASA physiques pour fournir des fonctionnalités de sécurité éprouvées dans un format virtuel. L'ASA virtuel peut être déployé dans le nuage AWS public. Il peut ensuite être configuré pour protéger les charges de travail des centres de données virtuels et physiques qui se développent, se contractent ou changent d'emplacement au fil du temps.

L'ASA virtuel prend en charge les types d'instances AWS suivants.

Tableau 13 : Types d'instances pris en charge par AWS

Instance	Attributs		Nombre maximal d'interfaces
	vCPU	Mémoire (Go)	
c3.large	2	3,75	3
c3.xlarge	4	7,5	4
c3.2xlarge	8	15	4
c4.large	2	3,75	3
c4.xlarge	4	7,5	4
c4.2xlarge	8	15	4
c5.large	2	4	3
c5.xlarge	4	8	4
c5.2xlarge	8	16	4
c5.4xlarge	16	32	8
c5a.large	2	4	3
c5a.xlarge	4	8	4
c5a.2xlarge	8	16	4
c5a.4xlarge	16	32	8
c5ad.large	2	4	3
c5ad.xlarge	4	8	4
c5ad.2xlarge	8	16	4
c5ad.4xlarge	16	32	8
c5d.large	2	4	3
c5d.xlarge	4	8	4
c5d.2xlarge	8	16	4
c5d.4xlarge	16	32	8
c5n.large	2	5,3	3
c5n.xlarge	4	10,5	4
c5n.2xlarge	8	21	4
c5n.4xlarge	16	42	8

Instance	Attributs		Nombre maximal d'interfaces
	vCPU	Mémoire (Go)	
m4.large	2	8	2
m4.xlarge	4	16	4
m4.2xlarge	8	32	4
m5n.large	2	8	3
m5n.xlarge	4	16	4
m5n.2xlarge	8	32	4
m5n.4xlarge	16	64	8
m5zn.large	2	8	3
m5zn.xlarge	4	16	4
m5zn.2xlarge	8	32	4

Astuces Si vous utilisez le type d'instance M4 ou C4, nous vous recommandons de migrer vers le type d'instance M5 ou C5 qui utilise des pilotes d'interface pour l'hyperviseur Nitro et Elastic Network Adapter (ENA) pour améliorer les performances.

Astuces Si vous utilisez le type d'instance C4, nous vous recommandons de migrer vers le type d'instance C5 qui utilise l'hyperviseur Nitro et les pilotes d'interface Elastic Network Adapter (ENA) pour améliorer les performances.

Tableau 14 : ASA virtuel Limites des fonctionnalités sous licence en fonction des droits

Niveau de performance	Type d'instance (cœur/RAM)	Limite du débit	Limite de session RA VPN
ASAv5	c5.large 2 cœurs/4 Go	100 Mbit/sec	50
ASAv10	c5.large 2 cœurs/4 Go	1 Gbit/sec	250
ASAv30	c5.xlarge 4 cœurs/8 Go	2 Gbit/s	750
ASAv50	c5.2xlarge 8 cœurs/16 Go	10 Gbit/s	10 000

Niveau de performance	Type d'instance (cœur/RAM)	Limite du débit	Limite de session RA VPN
ASAv100	c5n.4xlarge 16 cœurs/42 Go	16 Gbit/s	20 000

Vous créez un compte sur AWS, configurez l'ASA virtuel à l'aide de l'assistant AWS et avez choisi une image de machine Amazon (AMI). L'AMI est un modèle qui contient la configuration logicielle nécessaire pour lancer votre instance.

Important Les images d'AMI ne peuvent pas être téléchargées en dehors de l'environnement AWS.

Prérequis

- Créez un compte sur aws.amazon.com.
- Obtenez une licence pour l'ASA virtuel. Jusqu'à ce que vous obteniez une licence pour l'ASA virtuel, il fonctionnera en mode dégradé, ce qui n'autorisera que 100 connexions et un débit de 100 kbit/s. Consultez Gestion des licences pour l'ASA virtuel, à la page 1.
- Exigences d'interface :
  - Interface de gestion
  - Interfaces interne et externe
  - (Facultatif) Sous-réseau supplémentaire (DMZ)
- Chemins de communication :
  - Interface de gestion : utilisée pour connecter l'ASA virtuel à ASDM; ne peut pas être utilisée pour le trafic traversant.
  - Interface interne (requise) : utilisée pour connecter l'ASA virtuel aux hôtes internes.
  - Interface externe (requise) : utilisée pour connecter l'ASA virtuel au réseau public.
  - Interface DMZ (facultative) : utilisée pour connecter l'ASA virtuel au réseau DMZ lors de l'utilisation de l'interface c3.xlarge.
- Pour les exigences du système ASA virtuel, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

L'ASA virtuel sur AWS prend en charge les fonctionnalités suivantes :

- Prise en charge des instances Amazon EC2 C5, la prochaine génération de la famille d'instances de Calcul optimisé Amazon EC2.
- Déploiement dans le Cloud privé virtuel (VPC)
- Mise en réseau améliorée (SR-IOV), si disponible
- Déploiement à partir du Marché Amazon
- Déploiement des utilisateurs des réseaux L3
- Mode avec routeur (par défaut)
- Amazon CloudWatch

Fonctionnalités non prises en charge

L'ASA virtuel sur AWS ne prend pas en charge les éléments suivants :

- Accès à la console (la gestion est effectuée à l'aide de SSH ou ASDM sur les interfaces réseau)
- VLAN
- Mode promiscuité (pas de prise en charge de pare-feu en mode sniffer (analyseur de réseau) ou transparent)
- Mode contexte multiple
- Mise en grappes
- Haute disponibilité en natif ASA virtuel
- EtherChannel n'est pris en charge que sur les interfaces physiques directes
- Importation/exportation de machine virtuelle
- Package indépendant de l'hyperviseur
- VMware ESXi
- Messages de diffusion ou de multidiffusion

  Ces messages ne sont pas propagés dans AWS, de sorte que les protocoles de routage qui nécessitent la diffusion et la multidiffusion ne fonctionnent pas comme prévu dans AWS. VXLAN ne peut fonctionner qu'avec des homologues statiques.
- ARP Gratuitous et non sollicités

  Ces ARP ne sont pas acceptés dans AWS. Les configurations NAT qui nécessitent des ARP Gratuitous ou non sollicités ne fonctionnent pas comme prévu.
- IPv6

Migration de la configuration et authentification SSH

Incidence sur la mise à niveau lors de l'utilisation de l'authentification par clé publique SSH : en raison des mises à jour de l'authentification SSH, une configuration supplémentaire est requise pour activer l'authentification par clé publique SSH; par conséquent, les configurations SSH existantes utilisant

l'authentification par clé publique ne fonctionnent plus après la mise à niveau. L'authentification par clé publique est la valeur par défaut pour l'ASA virtuel sur Amazon Web Services (AWS), donc les utilisateurs AWS verront ce problème. Pour éviter la perte de connectivité SSH, vous pouvez mettre à jour votre configuration avant d'effectuer la mise à niveau. Vous pouvez également utiliser ASDM après la mise à niveau (si vous avez activé l'accès ASDM) pour corriger la configuration.

Voici un exemple de configuration d'origine pour un nom d'utilisateur « admin » :

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

Pour utiliser la commande **ssh authentication**, avant d'effectuer la mise à niveau, saisissez les commandes suivantes :

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

Nous vous recommandons de définir un mot de passe pour le nom d'utilisateur plutôt que de conserver le mot clé **nopassword**, s'il est présent. Le mot clé **nopassword** signifie que tout mot de passe peut être saisi, et non qu'aucun mot de passe ne peut être saisi. Dans les versions antérieures à la version 9.6(2), la commande **aaa** n'était pas requise pour l'authentification par clé publique SSH, le mot clé **nopassword** n'était donc pas déclenché. Maintenant que la commande **aaa** est requise, elle permet également l'authentification par mot de passe normale pour un mot clé **username** si le mot clé **password** (ou **nopassword**) est présent.

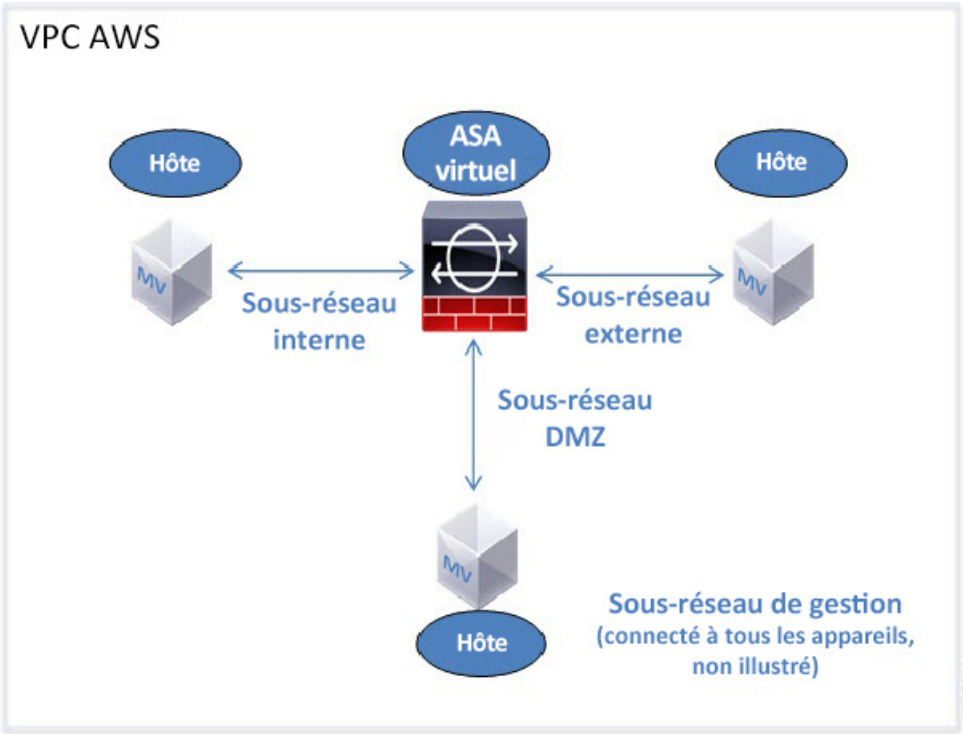
Après la mise à niveau, la commande **username** ne nécessite plus le mot clé **password** ou **nopassword**. Vous pouvez exiger qu'un utilisateur ne puisse pas saisir de mot de passe. Par conséquent, pour forcer l'authentification par clé publique uniquement, saisissez la commande **username** :

```
username admin privilege 15
```

Exemple de topologie de réseau

La figure suivante montre la topologie recommandée pour l'ASA virtuel en mode pare-feu routé avec quatre sous-réseaux configurés dans AWS pour l'ASA virtuel (gestion, interne, externe et DMZ).

Illustration 14 : Exemple d'ASA virtuel sur le déploiement AWS



Déploiement ASA virtuel

La procédure suivante fournit une liste de niveaux supérieurs des étapes pour configurer AWS sur l'ASA virtuel. Pour les étapes détaillées, consultez Mise en route d'AWS.

Procédure

Étape 1 Connectez-vous à aws.amazon.com et choisissez votre région.

Remarque
AWS est divisé en plusieurs régions isolées les unes des autres. Les régions sont affichées dans le coin supérieur droit de votre page. Les ressources disponibles dans une région n'apparaissent pas dans une autre région. Vérifiez périodiquement que vous êtes dans la région prévue.

Étape 2 Cliquez sur **My Account (Mon compte)** > **AWS Management Console (Console de gestion AWS)** et sous **Networking (Mise en réseau)**, cliquez sur **VPC** > **Start VPC Wizard (Démarrer l'assistant VPC)**, créez votre VPC en choisissant un seul sous-réseau public et configurez les éléments suivants (utilisez les paramètres par défaut, sauf indication contraire) :

- Sous-réseau interne et externe : saisissez un nom pour le VPC et les sous-réseaux.
- Passerelle Internet : saisissez le nom de la passerelle Internet. Elle permet la connectivité directe sur Internet.

- Table externe : ajoutez une entrée pour activer le trafic sortant vers Internet (ajoutez 0.0.0.0/0 à la passerelle Internet).

Étape 3 Cliquez sur **My Account (Mon compte)** > **AWS Management Console (Console de gestion AWS)** > **EC2**, puis sur **Create an Instance** (Créer une instance).

- Sélectionnez votre AMI, par exemple, le serveur Ubuntu 14.04 LTS.

  Utilisez l'AMI identifiée dans la notification de livraison de votre image.

- Choisissez le type d'instance pris en charge par l'ASA virtuel, par exemple, c3.large.
- Configurez l'instance (les CPU et la mémoire sont fixes).
- Développez la section **Advanced Details** (Détails avancés) et dans le champ **User data** (Données utilisateur) facultatif, vous pouvez saisir la configuration Day0 (Jour0), qui est le texte saisi contenant la configuration ASA virtuel appliquée lors du lancement d'ASA virtuel. Pour en savoir plus sur la configuration Day0 (Jour0), notamment sur les licences Smart, consultez la section Préparer le fichier de configuration Day0 (Jour0).
  - **Interface de gestion** : si vous choisissez de fournir les détails de la configuration Day0 (Jour0), vous *devez* fournir les détails de l'interface de gestion, qui doit être configurée pour utiliser DHCP.
  - **Interfaces de données** : les adresses IP des interfaces de données seront attribuées et configurées uniquement si vous fournissez ces renseignements dans le cadre de la configuration Day0 (Jour0). Les interfaces de données peuvent être configurées pour utiliser le protocole DHCP, ou si les interfaces réseau à associer sont déjà créées et les adresses IP connues, vous pouvez fournir les détails de l'adresse IP dans la configuration Day0 (Jour0).
  - **Sans configuration Day0 (Jour0)** : si vous déployez l'ASA virtuel *sans* fournir la configuration Day0 (Jour0), l'ASA virtuel applique la configuration ASA virtuel par défaut où il récupère les adresses IP des interfaces associées du serveur de métadonnées AWS et attribue les adresses IP (les interfaces de données obtiennent les adresses IP attribuées, mais les ENI seront inactifs). L'interface Management0/0 sera opérationnelle et obtiendra l'adresse IP configurée avec l'adresse DHCP. Consultez la section Adressage IP dans votre VPC pour en savoir plus sur Amazon EC2 et l'adressage IP d'Amazon VPC.

    Exemple de configuration Day0 (Jour0) -

```
! ASA Version 9.x.1.200
!
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shutdown
!


crypto key generate rsa modulus 2048
ssh 0 0 management
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Q1w2e3r4 privilege 15
username admin attributes
service-type admin
aaa authentication ssh console LOCAL
!
```

```
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute

no shutdown
!
interface G0/1
nameif inside
ip address dhcp

no shutdown
!
```

- Stockage : conservez les valeurs par défaut.
- Instance de balise : vous pouvez créer de nombreuses balises pour classer vos appareils. Attribuer un nom à vos appareils vous aide à les localiser facilement.
- Groupe de sécurité : créez un groupe de sécurité et nommez-le. Le groupe de sécurité est un pare-feu virtuel pour une instance permettant de contrôler le trafic entrant et sortant.

  Par défaut, le groupe de sécurité est ouvert à toutes les adresses. Modifiez les règles pour autoriser uniquement l'entrée SSH des adresses utilisées pour accéder à votre ASA virtuel.

  Pour savoir comment le groupe de sécurité contrôle le trafic, consultez la documentation d'AWS - Contrôler le trafic de vos ressources AWS à l'aide des groupes de sécurité.
- Développez la section **Advanced Details** (Détails avancés) et dans le champ **User data** (Données utilisateur), vous pouvez éventuellement saisir une configuration Day0 (Jour0), qui est le texte saisi contenant la configuration ASA virtuel appliquée lors du lancement d'ASA virtuel. Pour en savoir plus sur la façon de réaliser une configuration Day0 (Jour0), notamment sur les licences Smart, consultez la section Préparer le fichier de configuration Day0 (Jour0).
  - **Interface de gestion** : si vous choisissez de fournir une configuration Day0 (Jour0), vous **devez** fournir les détails de l'interface de gestion, qui doit être configurée pour utiliser DHCP.
  - **Interfaces de données** : les adresses IP des interfaces de données seront attribuées et configurées uniquement si vous fournissez ces renseignements dans le cadre de la configuration Day0 (Jour0). Les interfaces de données peuvent être configurées pour utiliser le protocole DHCP ou, si les interfaces réseau à associer sont déjà créées et que les adresses IP sont connues, vous pouvez fournir les détails de l'IP dans la configuration Day0 (Jour0).
  - **Sans configuration Day0 (Jour0)** : si vous déployez l'ASA virtuel **sans** fournir la configuration Day0 (Jour0), l'ASA virtuel applique la configuration ASA virtuel par défaut où il récupère les IP des interfaces associées du serveur de métadonnées AWS et attribue les IP (les interfaces de données obtiennent les IP attribuées, mais les ENI seront inactifs). L'interface Management0/0 sera opérationnelle et obtiendra l'IP configurée avec l'adresse DHCP. Consultez la section Adressage IP dans votre VPC pour en savoir plus sur Amazon EC2 et l'adressage IP d'Amazon VPC.
- Passez en revue votre configuration, puis cliquez sur **Launch** (Lancer).

Étape 4 Créez une paire de clés.

Mise en garde
Attribuez à la paire de clés un nom que vous reconnaîtrez et téléchargerez la clé en lieu sûr; la clé ne pourra jamais être téléchargée de nouveau. Si vous perdez la paire de clés, vous devez détruire vos instances et les redéployer.

Étape 5 Cliquez sur **Launch Instance** (Lancer l'instance) pour déployer votre ASA virtuel.

Étape 6 Cliquez sur **My Account (Mon compte)** > **AWS Management Console (Console de gestion AWS)** > **EC2** > **Launch an Instance (Lancer une instance)** > **My AMIs (Mes AMI)**.

Étape 7 Assurez-vous que la vérification de la source/destination est désactivée par interface pour l'ASA virtuel.

Les paramètres par défaut d'AWS permettent uniquement à une instance de recevoir le trafic pour son adresse IP (IPv4) et permettent uniquement à une instance d'envoyer le trafic de sa propre adresse IP (IPv4). Pour permettre à ASA virtuel d'agir comme un saut routé, vous devez désactiver la vérification de la source/destination sur chacune des interfaces de trafic d'ASA virtuel(interne, externe et DMZ).

Intégration du service Amazon GuardDuty et Défense contre les menaces virtuelles

Amazon GuardDuty est un service de supervision qui traite les données de diverses sources telles que les journaux VPC, les journaux des événements de gestion CloudTrail, les journaux des événements des données CloudTrail S3, les journaux DNS, etc. pour identifier les activités potentiellement non autorisées et malveillantes dans l'environnement AWS.

À propos de l'intégration d'Cisco Secure Firewall ASA virtuel et GuardDuty

Cisco propose une solution pour intégrer le service Amazon GuardDuty à Cisco Secure Firewall ASA virtuel à l'aide de l' interface de ligne de commande sur SSH.

Cette solution utilise les données ou les résultats d'analyse des menaces d'Amazon GuardDuty (adresses IP malveillantes générant des menaces, des attaques, etc.) et fournit ces informations (adresse IP malveillante) à l'Cisco Secure Firewall ASA virtuel pour protéger le réseau et les applications sous-jacentes contre les menaces futures provenant de ces sources (adresse IP malveillante).

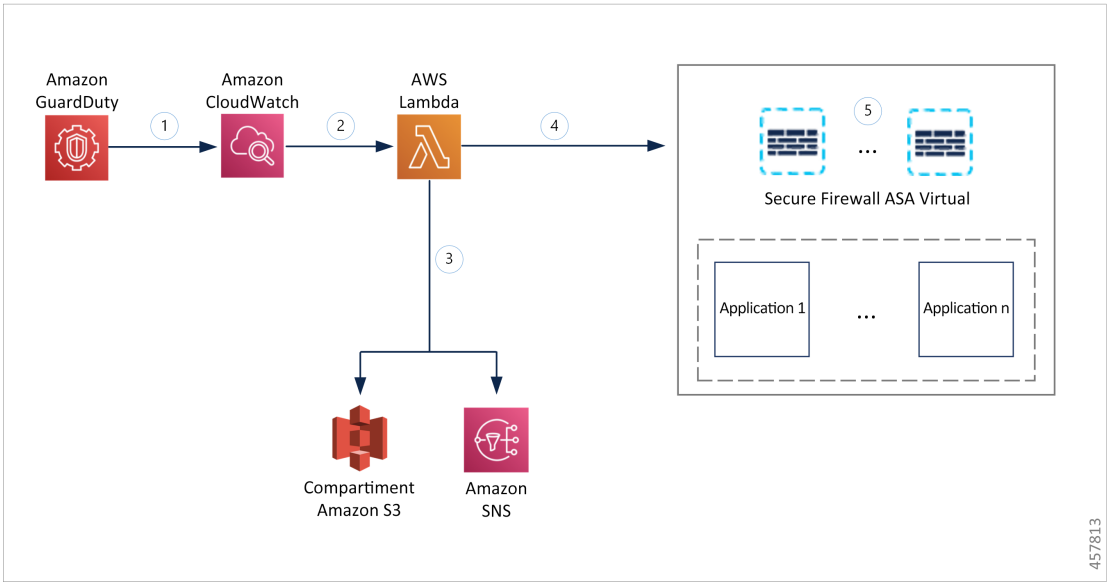
Procédure de bout en bout

Les solutions d'intégration suivantes avec des exemples de flux de travail vous aident à comprendre l'intégration d'Amazon GuardDuty avec Cisco Secure Firewall Threat Defense Virtual .

Le diagramme de flux de travail suivant montre la solution d'intégration d'Amazon GuardDuty avec ASA virtuel.

Intégration avec le Cisco Secure Firewall device manager à l'aide du groupe d'objets réseau

Le diagramme de flux de travail suivant montre la solution d'intégration d'Amazon GuardDuty avec le Cisco Secure Firewall device manager à l'aide du groupe d'objets réseau.



1	Le service GuardDuty envoie des résultats de menaces à CloudWatch lorsqu'il détecte une activité malveillante.
2	L'événement CloudWatch active la fonction Lambda d'AWS.
3	La fonction Lambda met à jour l'hôte malveillant dans le fichier de rapport dans le compartiment S3 et envoie une notification par SNS.
4	La fonction Lambda configure ou met à jour le groupe d'objets réseau avec l'adresse IP de l'hôte malveillant dans le Cisco Secure Firewall device manager.
5	La politique de contrôle d'accès du Cisco Secure Firewall device manager demande au périphérique géré de gérer le trafic en fonction des actions configurées, par exemple, bloquer le trafic des hôtes malveillants signalés par GuardDuty. Cette politique de contrôle d'accès utilise le groupe d'objets réseau avec l'adresse IP malveillante fournie par la fonction Lambda.

Composants clés de cette intégration

Composant	Description
Amazon GuardDuty	Un service Amazon responsable de la génération de résultats de menaces pour les diverses ressources AWS dans une région spécifique, comme EC2, S3, IAM, etc.

Amazon Simple Storage Service (S3)	Un service Amazon utilisé pour stocker divers artefacts associés à la solution : • Fichier zip de la fonction Lambda • Fichier zip de couche Lambda • Fichier d'entrée de la configuration (.ini) ASA virtuelde • Fichier de rapport de sortie (.txt) contenant une liste d'adresses IP malveillantes signalées par la fonction Lambda
Amazon CloudWatch	Un service Amazon utilisé pour : • Superviser le service GuardDuty pour détecter les résultats signalés et déclencher la fonction Lambda pour traiter les résultats. • Journalisation des activités liées à la fonction Lambda dans le groupe de journaux CloudWatch.
Amazon Simple Notification Service (SNS)	Un service Amazon utilisé pour envoyer des notifications par courriel. Ces notifications par courriel contiennent : • Les détails de résultat GuardDuty qui a été traité avec succès par la fonction Lambda. • Les détails des mises à jour effectuées sur les gestionnaires de Cisco Secure Firewall par la fonction Lambda. • Toutes les erreurs importantes rencontrées par la fonction Lambda.
Fonction AWS Lambda	Un service de traitement informatique sans serveur AWS qui exécute votre code en réponse aux événements et gère automatiquement les ressources de traitement sous-jacentes pour vous. La fonction Lambda est déclenchée par la règle d'événement CloudWatch en fonction des résultats de GuardDuty. Dans cette intégration, la fonction Lambda est responsable de : • Traitement des résultats de GuardDuty pour vérifier que tous les critères requis sont respectés, comme la gravité, le sens de la connexion, la présence d'adresses IP malveillantes, etc. • (Selon la configuration) Mise à jour du groupe d'objets réseau sur les gestionnaires de Cisco Secure Firewall avec l'adresse IP malveillante. • Mise à jour de l'adresse IP malveillante dans le fichier de rapport sur le compartiment S3. • Informer l'administrateur de Cisco Secure Firewall de différentes mises à jour de gestionnaire et de toute erreur.

Modèle CloudFormation	Utilisé pour déployer diverses ressources requises pour l'intégration dans AWS. Le modèle CloudFormation contient les ressources suivantes : • **AWS::SNS::Topic** : la rubrique SNS pour l'envoi de notifications par courriel. • **AWS::Lambda::Function, AWS::Lambda::LayerVersion** : la fonction Lambda et les fichiers de couche • **AWS::Events::Rule**: la règle d'événement CloudWatch pour déclencher la fonction Lambda en fonction de l'événement de résultats de GuardDuty. • **AWS::Lambda::Permission**: autorisation pour la règle d'événement CloudWatch de déclencher la fonction Lambda. • **AWS::IAM::Rôle, AWS::IAM::Policy** : le rôle et les ressources de politique IAM pour autoriser diverses autorisations d'accès à la fonction Lambda pour diverses ressources AWS. Ce modèle accepte les paramètres d'entrée des utilisateurs pour personnaliser le déploiement.

Plateformes logicielles prises en charge

- La solution d'intégration GuardDuty s'applique à Cisco Secure Firewall ASA virtuel géré à l'aide de l'interface de ligne de commande sur SSH.
- La fonction Lambda peut mettre à jour les groupes d'objets réseau dans le Cisco Secure Firewall ASA virtuel. Assurez-vous que la fonction Lambda peut se connecter à Cisco Secure Firewall ASA virtuel en utilisant des adresses IP publiques.

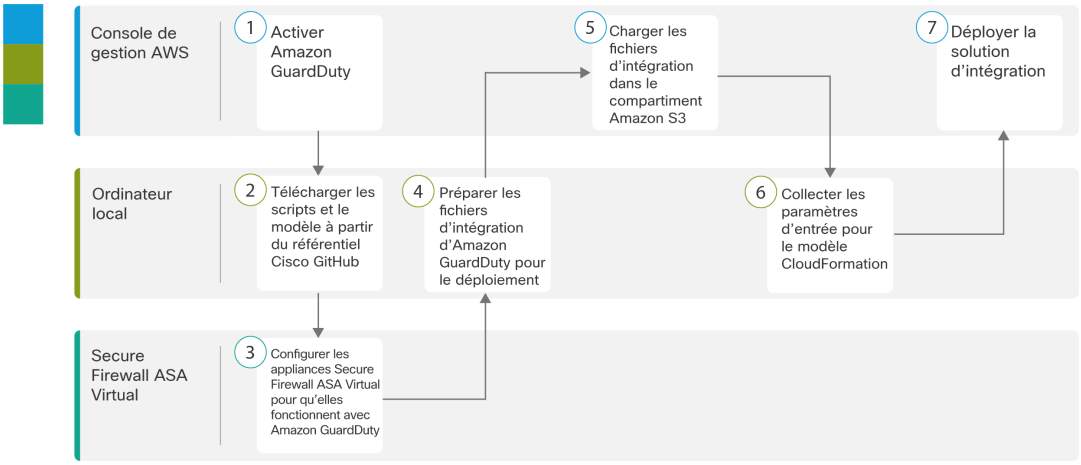
Lignes directrices et limites pour l'intégration d'Amazon GuardDuty et de Cisco Secure Firewall ASA Virtual

- La fonction Lambda est uniquement responsable de la mise à jour des groupes d'objets réseau avec les adresses IP malveillantes. Selon vos besoins, créez des règles d'accès et des politiques d'accès pour bloquer tout trafic non nécessaire.
- Les services AWS utilisés dans cette intégration sont propres à la région. Si vous souhaitez utiliser les résultats de GuardDuty de différentes régions, vous devez déployer des instances propres à la région.
- Vous pouvez configurer les mises à jour d'ASA virtuel à l'aide de l'interface de ligne de commande sur SSH. ASDM, CSM et CDO ne sont pas pris en charge.
- Vous pouvez uniquement utiliser la connexion par mot de passe. Aucune autre méthode d'authentification n'est prise en charge.
- Si vous utilisez des mots de passe chiffrés dans le fichier d'entrée, gardez à l'esprit que :
    - Seul le chiffrement à l'aide des clés KMS symétriques est pris en charge.

- Tous les mots de passe doivent être chiffrés à l'aide d'une clé KMS unique accessible à la fonction Lambda.

Intégrer Amazon GuardDuty avec ASA virtuel

Effectuer les tâches suivantes pour intégrer Amazon GuardDuty à ASA virtuel



	Espace de travail	Étapes
1	Console de gestion AWS	Activer le service Amazon GuardDuty sur AWS, à la page 88
2	Ordinateur local	Télécharger le Cisco Secure Firewall ASA virtuel et le modèle de solution Amazon GuardDuty, à la page 89
3	ASA virtuel	Configurer vos périphériques gérés pour qu'ils fonctionnent avec Amazon GuardDuty, à la page 90
4	Ordinateur local	Préparer les fichiers de ressources d'Amazon GuardDuty pour le déploiement, à la page 92
5	Console de gestion AWS	Charger des fichiers dans le service Amazon Simple Storage, à la page 95
6	Ordinateur local	Collecter les paramètres d'entrée pour le modèle CloudFormation, à la page 96
7	Console de gestion AWS	Déployer la pile, à la page 98

Activer le service Amazon GuardDuty sur AWS

Cette section décrit comment activer le service Amazon GuardDuty sur AWS.

Avant de commencer

Assurez-vous que toutes les ressources AWS se trouvent dans la même région.

Procédure

Étape 1 Accédez à https://aws.amazon.com/marketplace (Amazon Marketplace) et connectez-vous.

Étape 2 Choisissez **Services** > **GuardDuty**.

Étape 3 Cliquez sur **Get Started** (Mise en route) dans la page **GuardDuty**.

Étape 4 Cliquez sur **Enable GuardDuty** (Activer GuardDuty) pour activer le service Amazon GuardDuty.

Pour en savoir plus sur l'activation de GuardDuty, consultez la section Mise en route de GuardDuty dans la documentation d'AWS.

Prochaine étape

Téléchargez les fichiers de solution Amazon GuardDuty (modèles et scripts) à partir du référentiel Cisco GitHub. Consultez .Télécharger le Cisco Secure Firewall ASA virtuel et le modèle de solution Amazon GuardDuty, à la page 89

Télécharger le Cisco Secure Firewall ASA virtuel et le modèle de solution Amazon GuardDuty

Téléchargez les fichiers requis pour la solution Amazon GuardDuty. Les scripts et les modèles de déploiement pour votre version de Cisco Secure Firewall ASA virtuel sont disponibles dans le référentiel Cisco GitHub à l'adresse :

https://github.com/CiscoDevNet/cisco-asav

Voici une liste de ressources dans le référentiel Cisco GitHub :

Fichiers	Description
READ.MD	Fichier ReadMe
configuration/	Modèle de fichier de configuration d'Cisco Secure Firewall ASA virtuel.
images/	Il contient l'Cisco Secure Firewall ASA virtuel et des exemples de solutions d'intégration Amazon GuardDuty.
lambda/	Fichiers Python de fonction Lambda.
templates/	Modèle CloudFormation pour le déploiement.

Configurer vos périphériques gérés pour qu'ils fonctionnent avec Amazon GuardDuty

La fonction Lambda traite les résultats d'Amazon GuardDuty et identifie l'adresse IP malveillante qui a déclenché l'événement CloudWatch. Ensuite, la fonction Lambda met à jour le groupe d'objets réseau dans l'ASAv avec l'adresse IP malveillante. Vous pouvez ensuite configurer une stratégie de contrôle d'accès qui utilise ce groupe d'objets réseau pour gérer le trafic.

Créer un groupe d'objets réseau

Dans ASA virtuel, vous devez configurer ou créer un groupe d'objets réseau pour la fonction Lambda afin de mettre à jour l'adresse IP malveillante détectée par Amazon GuardDuty.

Si vous ne configurez pas de groupe d'objets réseau avec la fonction Lambda, un groupe d'objets réseau avec le nom par défaut **aws-gd-suspicious-hosts** est créé par la fonction Lambda pour mettre à jour l'adresse IP malveillante.

Créer un groupe d'objets réseau dans Cisco Secure Firewall ASA Virtual

Dans Cisco Secure Firewall ASA Virtual, vous devez créer un groupe d'objets réseau pour la fonction Lambda afin de mettre à jour l'adresse IP malveillante détectée par Amazon GuardDuty.

Si vous ne configurez pas de groupe d'objets réseau avec la fonction Lambda, un groupe d'objets réseau avec le nom par défaut *aws-gd-suspicious-hosts* est créé par la fonction Lambda pour mettre à jour l'adresse IP malveillante.

Initialement, pour utiliser le groupe d'objets réseau dans une règle ACL, vous devrez peut-être créer le groupe d'objets avec une adresse IP factice. Vous pouvez créer plusieurs groupes d'objets réseau sur un seul ASAv.

Pour en savoir plus sur le groupe d'objets réseau et la politique d'accès, consultez le guide de configuration de l'interface de ligne de commande des pare-feu de la série Cisco ASA.

Pour créer le groupe d'objets réseau, procédez comme suit :

Procédure

Étape 1 Connectez-vous à Cisco Secure Firewall ASA Virtual.

Étape 2 Créez un groupe d'objets réseau avec une description. Dans cet exemple, une adresse IP d'hôte factice 12.12.12.12 est ajoutée au groupe d'objets réseau créé.

Exemple :

```
hostname(config)# object-group network aws-gd-suspicious-hosts
hostname(config)# description Malicious Hosts reported by AWS GuardDuty
hostname(config)# network-object host 12.12.12.12
```

Étape 3 Créez ou mettez à jour la politique d'accès ou la règle de contrôle d'accès pour gérer le trafic à l'aide du groupe d'objets réseau. \

Astuces
Vous pouvez également créer ou mettre à jour la politique de contrôle d'accès ou la règle de contrôle d'accès après avoir vérifié que la fonction Lambda met à jour le groupe d'objets réseau avec l'adresse IP malveillante.

Exemple :

```
hostname(config)# access-list out-iface-access line 1 extended deny ip object-group
aws-gd-suspicious-hosts any
```

Création de comptes d'utilisateur dans ASAv pour l'accès à la fonction Lambda

La fonction Lambda nécessite un utilisateur dédié sur ASAv pour gérer les mises à jour de configuration. Un niveau de privilège de 15 garantit que l'utilisateur dispose de tous les privilèges.

Pour en savoir plus sur la création d'utilisateur, consultez le guide de configuration de l'interface de ligne de commande des pare-feu de la série Cisco ASA.

Procédure

Étape 1 Créez un utilisateur.

username *nom* [**password** *mot de passe*] **privilege** *niveau*

Exemple :

```
hostname(config)# username aws-gd password MyPassword@2021 privilege 15
```

Étape 2 Configurez les attributs de nom d'utilisateur.

username *nom d'utilisateur* **attributes**

Exemple :

```
hostname(config)# username aws-gd attributes
```

Étape 3 Fournissez à l'utilisateur un accès de niveau administrateur à tous les services.

service-type admin

Exemple :

```
hostname(config)# service-type admin
```

(Facultatif) Chiffrer les mots de passe

Au besoin, vous pouvez fournir des mots de passe chiffrés dans le fichier de configuration d'entrée. Vous pouvez également fournir des mots de passe en texte brut.

Chiffrez tous les mots de passe à l'aide d'une clé KMS unique accessible à la fonction Lambda. Utilisez la commande **aws kms encrypt --key-id** <*KMS-ARN*> **--plaintext** <*password*> pour générer le mot de passe chiffré. Vous devez installer et configurer l'interface de ligne de commande AWS pour exécuter cette commande.

Remarque Assurez-vous que les mots de passe sont chiffrés à l'aide de clés KMS symétriques.

Pour en savoir plus sur l'interface de ligne de commande AWS, consultez Interface de ligne de commande AWS. Pour en savoir plus sur les clés principales et le chiffrement, consultez le document AWS Création de clés et la Référence de commande de l'interface de ligne de commande AWS sur le chiffrement des mots de passe et KMS.

Exemple :

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext <password>
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

La valeur de la clé *CiphertextBlob* doit être utilisée comme mot de passe.

Préparer les fichiers de ressources d'Amazon GuardDuty pour le déploiement

Les fichiers de ressources de déploiement de la solution Amazon GuardDuty sont disponibles dans le référentiel Cisco GitHub.

Avant de déployer la solution Amazon GuardDuty sur AWS, vous devez préparer les fichiers suivants :

- Fichier d'entrée de configuration du gestionnaire Secure Firewall ASA virtuel
- Fichier zip de la fonction Lambda
- Fichier zip de la couche Lambda

Préparer le fichier d'entrée de la configuration

Dans le modèle de configuration, vous devez définir les détails de l'ASAv que vous intégrez à la solution Amazon GuardDuty.

Avant de commencer

- Assurez-vous d'authentifier et de vérifier le compte d'utilisateur du gestionnaire d'appareils avant de fournir les détails du compte d'utilisateur dans le fichier de configuration.
- Assurez-vous de configurer un seul ASAv dans le fichier de configuration. Si vous configurez plusieurs ASAv, la fonction Lambda peut mettre à jour simultanément tous les ASAv configurés dans le fichier, ce qui entraîne une situation de concurrence et un comportement déterministe.
- Vous devez avoir noté l'adresse IP et le nom de l'ASAv.
- Vous devez avoir créé un compte d'utilisateur disposant de privilèges d'administrateur pour la fonction Lambda afin d'accéder à ces groupes d'objets réseau dans l'ASAv et de les mettre à jour.

Procédure

Étape 1 Connectez-vous à la machine locale sur laquelle vous avez téléchargé les fichiers de ressources Amazon GuardDuty.

Étape 2 Accédez au dossier **asav-template** > **configuration**.

Étape 3 Ouvrez le fichier `asav-manager-config-input.ini` dans un éditeur de texte. Dans ce fichier, vous devez saisir les détails de l'ASAv sur lequel vous prévoyez d'intégrer et de déployer la solution Amazon GuardDuty.

Étape 4 Entrez les paramètres ASAv suivants :

Paramètres	Description
[asav-1]	Nom de la section : identifiant ASAv unique dans le fichier
public-ip	Adresse IP publique de l'ASAv
user name	Nom d'utilisateur pour se connecter à l'ASAv.
mot de passe	Mot de passe de connexion à l'ASAv. Le mot de passe peut être en texte brut ou une chaîne chiffrée qui a été chiffrée à l'aide de KMS.
enable-password	Activer le mot de passe de l'ASAv. Le mot de passe peut être en texte brut ou une chaîne chiffrée qui a été chiffrée à l'aide de KMS.
object-group-name	Nom de groupes d'objets réseau mis à jour avec l'adresse IP d'hôte malveillante par la fonction Lambda. Si vous saisissez plusieurs noms de groupes d'objets réseau, assurez-vous qu'il s'agit de valeurs séparées par des virgules.

Étape 5 Enregistrez et fermez le fichier `asav-manager-config-input.ini`.

Prochaine étape

Créez le fichier d'archive de la fonction Lambda.

Préparation du fichier d'archive de la fonction Lambda

Cette section décrit comment archiver les fichiers de fonction Lambda dans un environnement Linux.

Remarque Le processus d'archivage peut différer selon le système d'exploitation de la machine locale sur laquelle vous archivez les fichiers.

Avant de commencer

Assurez-vous que votre hôte Linux exécute Ubuntu version 18.04 avec Python version 3.6 ou ultérieure.

Procédure

Étape 1 Ouvrez la console d'interface en ligne de commande sur la machine locale sur laquelle vous avez téléchargé les ressources d'Amazon GuardDuty.

Étape 2 Accédez au dossier /lambda et archivez les fichiers. Voici un exemple de transcription à partir d'un hôte Linux.

```
$ cd lambda
$ zip asav-gd-lambda.zip *.py
adding: aws.py (deflated 71%)
adding: asav.py (deflated 79%)
adding: main.py (deflated 73%)
adding: utils.py (deflated 65%)
$
```

Le fichier zip `asav-gd-lambda.zip` est créé.

Étape 3 Quittez et fermez la console d'interface en line de commande.

Prochaine étape

Créez le fichier zip de couche Lambda à l'aide du fichier zip `asav-gd-lambda.zip`.

Préparer le fichier de la couche Lambda

Cette section décrit comment archiver le fichier de la couche Lambda dans un environnement Linux.

Remarque Le processus d'archivage peut différer selon le système d'exploitation de la machine locale sur laquelle vous archivez le fichier.

Procédure

Étape 1 Ouvrez la console d'interface en ligne de commande de la machine locale sur laquelle vous avez téléchargé les ressources d'Amazon GuardDuty.

Étape 2 Effectuez les actions suivantes dans votre console d'interface en ligne de commande.

Voici un exemple de transcription à partir d'un hôte Linux tel qu'Ubuntu 22.04 avec Python 3.9 installé.

```
$ mkdir -p layer
$ virtualenv -p /usr/bin/python3.9 ./layer/
$ source ./layer/bin/activate
$ pip3.9 install cffi==1.15.0
$ pip3.9 install cryptography==37.0.2
$ pip3.9 install paramiko==2.7.1
$ mkdir -p ./python/.libs_cffi_backend/
$ cp -r ./layer/lib/python3.9/site-packages/* ./python/
$ zip -r asav-gd-lambda-layer.zip ./python
```

Le fichier zip `asav-gd-lambda-layer.zip` est créé.

Notez que vous devez installer Python 3.9 et ses dépendances pour créer la couche Lambda.

Voici l'exemple de transcription pour l'installation de Python 3.9 sur un hôte Linux tel qu'Ubuntu 22.04.

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

Étape 3 Quittez et fermez la console d'interface en line de commande.

Prochaine étape

Dans le compartiment Amazon S3, vous devez charger le fichier de configuration Secure Firewall ASA virtuel, le fichier zip de la fonction Lambda et le fichier zip de la couche Lambda. Voir la section Charger des fichiers dans le service Amazon Simple Storage, à la page 95.

Charger des fichiers dans le service Amazon Simple Storage

Après avoir préparé tous les artefacts de solution Amazon GuardDuty, vous devez charger les fichiers dans un dossier de compartiment Amazon Simple Storage Service (S3) dans le portail AWS.

Procédure

Étape 1 Accédez à https://aws.amazon.com/marketplace (Amazon Marketplace) et connectez-vous.

Étape 2 Ouvrez la console Amazon S3.

Étape 3 Créez un compartiment Amazon S3 pour le chargement des artefacts Amazon GuardDuty. Consultez Création d'Amazon S3.

Étape 4 Chargez les artefacts Amazon GuardDuty suivants dans le compartiment Amazon S3.

- Fichier de configuration de Cisco Secure Firewall ASA virtuel : `asav-config-input.ini`

  Remarque
  Il n'est pas nécessaire de charger ce fichier lorsque vous utilisez la méthode Security Intelligence Network Feed (flux de réseau de renseignements de sécurité) pour le déploiement de la solution Amazon GuardDuty dans les centres de gestion.

- Fichier zip de la couche Lambda : `asav-gd-lambda-layer.zip`
- Fichier zip de la fonction Lambda : `asav-gd-lambda.zip`

Prochaine étape

Préparez le modèle CloudFormation utilisé pour le déploiement des ressources d'Amazon GuardDuty. Consultez Collecter les paramètres d'entrée pour le modèle CloudFormation, à la page 96.

Collecter les paramètres d'entrée pour le modèle CloudFormation

Cisco fournit le modèle CloudFormation utilisé pour déployer les ressources requises par la solution Amazon GuardDuty dans AWS. Collectez des valeurs pour les paramètres de modèle suivants avant le déploiement.

Procédure

Template Parameters

Paramètre	Description	Exemple
Nom du déploiement*	Le nom que vous saisissez dans ce paramètre est utilisé comme préfixe pour toutes les ressources créées par le modèle CloudFormation.	**cisco-asav-gd**
Niveau de gravité minimal de la recherche de GD*	Le niveau de gravité minimal des résultats d'Amazon GuardDuty à prendre en compte pour le traitement doit être compris entre **1,0** et **8,9**. Tout résultat signalé avec une gravité inférieure à la plage minimale est ignoré. La classification de la gravité est la suivante : • Faible : de 1,0 à 3,9 Moyenne : de 4,0 à 6,9 Élevée : de 7,0 à 8,9	**4,0**
ID d'e-mail de l'administrateur*	Adresse e-mail de l'administrateur pour recevoir des notifications sur Secure Firewall ASA virtuel au sujet des mises à jour effectuées par la fonction Lambda dans le Secure Firewall ASA virtuel.	**abc@xyz.com**
Nom du compartiment S3*	Nom du compartiment Amazon S3 contenant les fichiers d'artefacts Amazon GuardDuty (fichier zip de la fonction Lambda, fichier zip de la couche Lambda et fichiers de gestionnaire de configuration Secure Firewall ASA virtuel).	Par exemple : **asav-gd-bucket**

Paramètre	Description	Exemple
Préfixe de dossier/chemin d'accès au compartiment S3	Chemin d'accès au compartiment Amazon S3 ou nom du dossier dans lequel les fichiers de configuration sont stockés. S'il n'y a pas de dossier, laissez ce champ vide.	Par exemple : **« »** ou « **cisco/asav-gd/** »
Nom du fichier zip de la couche Lambda*	Nom du fichier zip de la couche Lambda.	Par exemple : `asav-gd-lambda-layer.zip`
Nom du fichier zip de la fonction Lambda*	Nom du fichier zip de la fonction Lambda.	Par exemple : `asav-gd-lambda.zip`
Secure Firewall ASA virtuel	Le fichier ***.ini** contenant les détails de configuration du gestionnaire Secure Firewall ASA virtuel. (Adresse IP publique, nom d'utilisateur, mot de passe, type d'appareil, noms de groupes d'objets réseau, etc.)	Par exemple : `asav-config-input.ini`
ARN de la clé KMS utilisée pour le chiffrement des mots de passe	ARN d'une clé KMS existante (clé KMS AWS utilisée pour le chiffrement des mots de passe). Vous pouvez laisser ce paramètre vide dans le cas où des mots de passe en texte brut sont fournis dans le fichier d'entrée de configuration de Secure Firewall ASA virtuel. Si vous le spécifiez, tous les mots de passe mentionnés dans le fichier d'entrée de la configuration de Secure Firewall ASA virtuel doivent être chiffrés. Les mots de passe doivent être chiffrés uniquement à l'aide de l'ARN spécifié. Génération de mots de passe chiffrés : aws kms encrypt --key-id <ARN KMS> --plaintext <password>	Par exemple : **arn:aws:kms:<region>:<awsaccountid>:key/<keyid>**
Activer/désactiver les journaux de débogage*	Activez ou désactivez les journaux de débogage de la fonction Lambda dans CloudWatch.	Par exemple : **activer** ou **désactiver**

* : Champ obligatoire

Prochaine étape

Déployez la pile à l'aide du modèle CloudFormation. Voir la section Déployer la pile, à la page 98.

Déployer la pile

Une fois que toutes les conditions préalables pour le déploiement de la solution Amazon GuardDuty sont terminées, créez la pile AWS CloudFormation. Utilisez le fichier de modèle dans le répertoire cible : `templates/cisco-asav-gd-integration.yaml`, et fournissez les paramètres collectés dans Collect Input Parameters for CloudFormation Template (Recueillir les paramètres d'entrée pour le modèle CloudFormation).

Procédure

Étape 1 Connectez-vous à la console AWS.

Étape 2 Accédez à Services > CloudFormation > Stacks (Piles) > Create stack (Créer une pile) (avec de nouvelles ressources) > Prepare template (Préparer le modèle) (le modèle est fourni dans le dossier) > Specify template (Spécifier le modèle) > Template source (Source du modèle) (chargez le fichier de modèle à partir du répertoire cible : `templates/cisco-asav-gd-integration.yaml`) > Create Stack (Créer une pile).

Pour en savoir plus sur le déploiement d'une pile sur AWS, consultez la documentation d'AWS.

Prochaine étape

Validez votre déploiement. Consultez Valider votre déploiement, à la page 99.

Abonnez-vous également pour recevoir des notifications par e-mail sur les mises à jour de détection des menaces signalées par Amazon GuardDuty. Consultez S'abonner aux notifications par courriel, à la page 98.

S'abonner aux notifications par courriel

Dans le modèle CloudFormation, un identifiant de courriel est configuré pour recevoir des notifications sur les mises à jour des résultats de GuardDuty effectuées par la fonction Lambda. Après avoir déployé le modèle CloudFormation sur AWS, une notification par courriel est envoyée à cet identifiant de courriel par le biais du service Amazon Web Notification Service (SNS) vous demandant de vous abonner pour recevoir les mises à jour de notification.

Procédure

Étape 1 Ouvrez la notification par courriel :

Étape 2 Cliquez sur le lien **Subscription** (abonnement) disponible dans la notification par courriel.

Prochaine étape

Validez votre déploiement. Consultez Valider votre déploiement, à la page 99.

Valider votre déploiement

Dans AWS, vous avez des options pour vérifier la solution Amazon GuardDuty, comme décrit dans cette section. Vous pouvez suivre ces instructions de validation du déploiement une fois le déploiement de CloudFormation terminé.

Avant de commencer

Assurez-vous d'avoir installé et configuré l'interface de ligne de commande (CLI) AWS pour exécuter des commandes de validation du déploiement. Pour en savoir plus sur la documentation relative à l'interface de ligne de commande AWS, consultez Interface de ligne de commande AWS.

Procédure

Étape 1 Connectez-vous à la console de gestion AWS.

Étape 2 Accédez à **Services > GuardDuty > Settings (Paramètres) > About GuardDuty (À propos de GuardDuty) > Detector ID (ID de détecteur)** pour noter l'ID de détecteur.

Cet ID de détecteur est requis pour générer des exemples de résultats dans Amazon GuardDuty.

Étape 3 Ouvrez la console d'interface en ligne de commande AWS pour générer l'exemple de résultat dans Amazon GuardDuty en exécutant les commandes suivantes :

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

Étape 4 Vérifiez l'exemple de résultat dans la liste des résultats sur la console Amazon GuardDuty.

Les exemples de résultats contiennent le préfixe **[sample]** (exemple). Vous pouvez vérifier les détails de l'exemple de résultat en affichant les attributs tels que le sens de connexion, l'adresse IP distante, etc.

Étape 5 Attendez que la fonction Lambda s'exécute.

Après le déclenchement de la fonction Lambda, vérifiez les éléments suivants :

- Une notification par e-mail avec les détails concernant les résultats d'Amazon GuardDuty reçus et les mises à jour de Secure Firewall ASA virtuel effectuées par la fonction Lambda.
- Vérifiez si le fichier de rapport est généré dans le compartiment Amazon S3. Il contient l'adresse IP malveillante signalée par l'exemple de résultat dans Amazon GuardDuty. Vous pouvez identifier le nom du fichier de rapport au format : `<deployment-name>-report.txt`.
- vérifiez que les groupes d'objets réseau sont mis à jour sur les gestionnaires configurés (Secure Firewall ASA virtuel) avec l'adresse IP malveillante mise à jour à partir de l'exemple de résultat.

Étape 6 Accédez à **AWS Console (Console AWS) > Services > CloudWatch > Logs (Journaux) > Log groups (Groupes de journaux) >** *select the log group (sélectionner le groupe de journaux)* pour vérifier les journaux Lambda dans la console CloudWatch. Vous pouvez identifier le nom du groupe de journaux CloudWatch au format : `<deployment-name>-lambda`.

Étape 7 Après avoir validé le déploiement, nous vous recommandons de nettoyer les données générées par l'exemple de résultat comme suit :

a) Accédez à **AWS Console (Console AWS) > Services > GuardDuty > Findings (Résultats) > Select the finding (Sélectionner le résultat) > Actions > Archive (Archiver)** pour afficher les exemples de données de résultat.
b) Supprimez les adresses IP malveillantes ajoutées dans le groupe d'objets réseau pour effacer les données mises en mémoire cache de Secure Firewall ASA virtuel.
c) Nettoyez le fichier de rapport dans le compartiment Amazon S3. Vous pouvez mettre à jour le fichier en supprimant les adresses IP malveillantes signalées par l'exemple de résultat.

Mettre à jour la configuration de déploiement de solution existante

Nous vous recommandons de ne pas mettre à jour le compartiment S3 ou les valeurs de préfixe de dossier et de chemin d'accès au compartiment S3 après le déploiement. Toutefois, si vous devez mettre à jour la configuration d'une solution qui a été déployée, utilisez l'option **`Update Stack`** (Mettre à jour la pile) sur la page CloudFormation dans la console AWS.

Vous pouvez mettre à jour n'importe lequel des paramètres ci-dessous.

Paramètre	Description
Nom du fichier de configuration du gestionnaire Secure Firewall ASA virtuel	Ajoutez ou mettez à jour le fichier de configuration dans le compartiment Amazon S3. Vous êtes autorisé à mettre à jour le fichier du même nom que le fichier précédent. Si le nom du fichier de configuration est modifié, vous pouvez mettre à jour ce paramètre en utilisant l'option **Update stack** (Mettre à jour la pile) dans la console AWS.
Niveau de gravité minimal de la recherche de GD*	Utilisez l'option **Update stack** (Mettre à jour la pile) dans la console AWS pour mettre à jour la valeur du paramètre.
ID d'e-mail de l'administrateur*	Mettez à jour la valeur du paramètre d'ID d'e-mail à l'aide de l'option **Update Stack** (Mettre à jour la pile) dans la console AWS. Vous pouvez également ajouter ou mettre à jour des abonnements par e-mail via la console de service SNS.
Nom du compartiment S3*	Mettez à jour le fichier zip dans le compartiment Amazon S3 avec un nouveau nom, puis mettez à jour le paramètre à l'aide de l'option **Update Stack** (Mettre à jour la pile) dans la console AWS.
Nom du fichier zip de la couche Lambda*	Mettez à jour le nom du fichier zip de la couche Lambda dans le compartiment Amazon S3 avec un nouveau nom, puis mettez à jour cette valeur de paramètre à l'aide de l'option **Update Stack** (Mettre à jour la pile) dans la console AWS.

Paramètre	Description
Nom du fichier zip de la fonction Lambda*	Mettez à jour le fichier zip de la fonction Lambda dans le compartiment Amazon S3 avec un nouveau nom, puis mettez à jour cette valeur de paramètre à l'aide de l'option **Update Stack** (Mettre à jour la pile) dans la console AWS.
ARN de la clé KMS utilisée pour le chiffrement des mots de passe	Utilisez l'option **Update stack** (Mettre à jour la pile) dans la console AWS pour mettre à jour la valeur du paramètre.
Activer/désactiver les journaux de débogage*	Utilisez l'option **Update stack** (Mettre à jour la pile) dans la console AWS pour mettre à jour la valeur du paramètre.

Procédure

Étape 1 Accédez à la console de gestion AWS.

Étape 2 Si nécessaire, créez le nouveau compartiment et le nouveau dossier.

Étape 3 Assurez-vous que les artefacts ci-dessous sont copiés de l'ancien compartiment au nouveau compartiment.

- Fichier de configuration de Cisco Secure Firewall ASA virtuel : `asav-config-input.ini`
- Fichier zip de la couche Lambda : `asav-gd-lambda-layer.zip`
- Fichier zip de la fonction Lambda : `asav-gd-lambda.zip`
- Fichier de rapport de sortie : `<deployment-name>-report.txt`

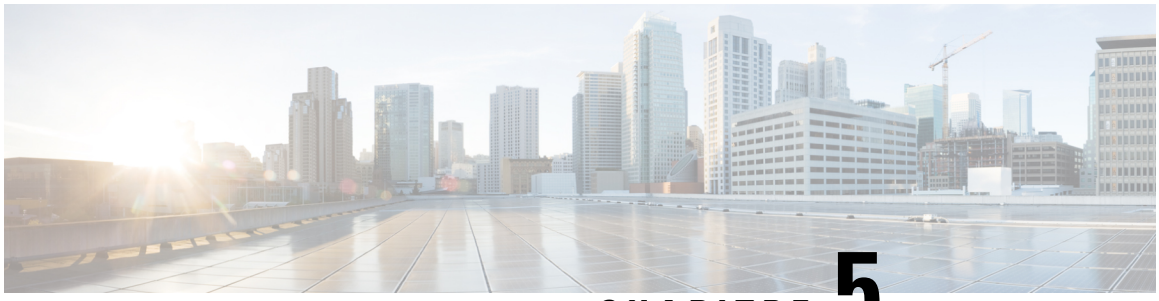
Étape 4 Pour mettre à jour les valeurs des paramètres, accédez à **Services > CloudFormation > Stacks > > Update (Update Stack) > Prepare template > Use current template > Next >** <*update parameters*>> **Update Stack**.

Réglage de la performance

Optimisation du réseau privé virtuel (VPN)

Les instances AWS c5 offrent des performances beaucoup plus élevées que les anciennes instances c3, c4 et m4. Le débit approximatif du VPN d'accès à distance (DTLS utilisant un trafic TCP de 450B avec le chiffrement AES-CBC) sur la famille d'instances c5 devrait être :

- 0,5 Gbit/s sur c5.large
- 1 Gbit/s sur c5.xlarge
- 2 Gbit/s sur c5.2xlarge



CHAPITRE 5

Déployer la solution d'évolutivité automatique ASA virtuel sur AWS

- Solution d'évolutivité automatique pour la Défense contre les menaces virtuelles ASA virtuel sur AWS , à la page 103
- Prérequis, à la page 106
- Déployer la solution d'évolutivité automatique, à la page 109
- Tâches de maintenance, à la page 117
- Dépannage et débogage , à la page 120

Solution d'évolutivité automatique pour la Défense contre les menaces virtuelles ASA virtuel sur AWS

Les sections suivantes décrivent comment les composants de la solution d'évolutivité automatique fonctionnent pour la ASA virtuel sur AWS.

Aperçu

Cisco fournit des modèles et des scripts CloudFormation pour le déploiement d'un groupe d'évolutivité automatique de pare-feu ASA virtuel à l'aide de plusieurs services AWS, notamment Lambda, les groupes d'évolutivité automatique, Elastic Load Balancing (ELB, équilibreur de charge élastique), les compartiments Amazon S3, SNS et CloudWatch.

L'évolutivité automatique de l'ASA virtuel dans AWS est une implémentation complète sans serveur (c.-à-d. aucune machine virtuelle d'assistant n'est impliquée dans l'automatisation de cette fonctionnalité) qui ajoute une capacité d'évolutivité automatique horizontale aux instances d'ASA virtuel dans l'environnement AWS. À partir de la version 6.4, la solution d'évolutivité automatique est prise en charge sur gérée par centre de gestion.

La solution d'évolutivité automatique ASA virtuel est un déploiement basé sur un modèle CloudFormation qui fournit :

- La configuration entièrement automatisée s'applique automatiquement aux instances ASA virtuel mises à l'échelle.
- Prise en charge des équilibreurs de charge et des zones de multi disponibilité.

- Prise en charge de l'activation et de la désactivation de la fonction d'évolutivité automatique.

Scénario d'évolutivité automatique

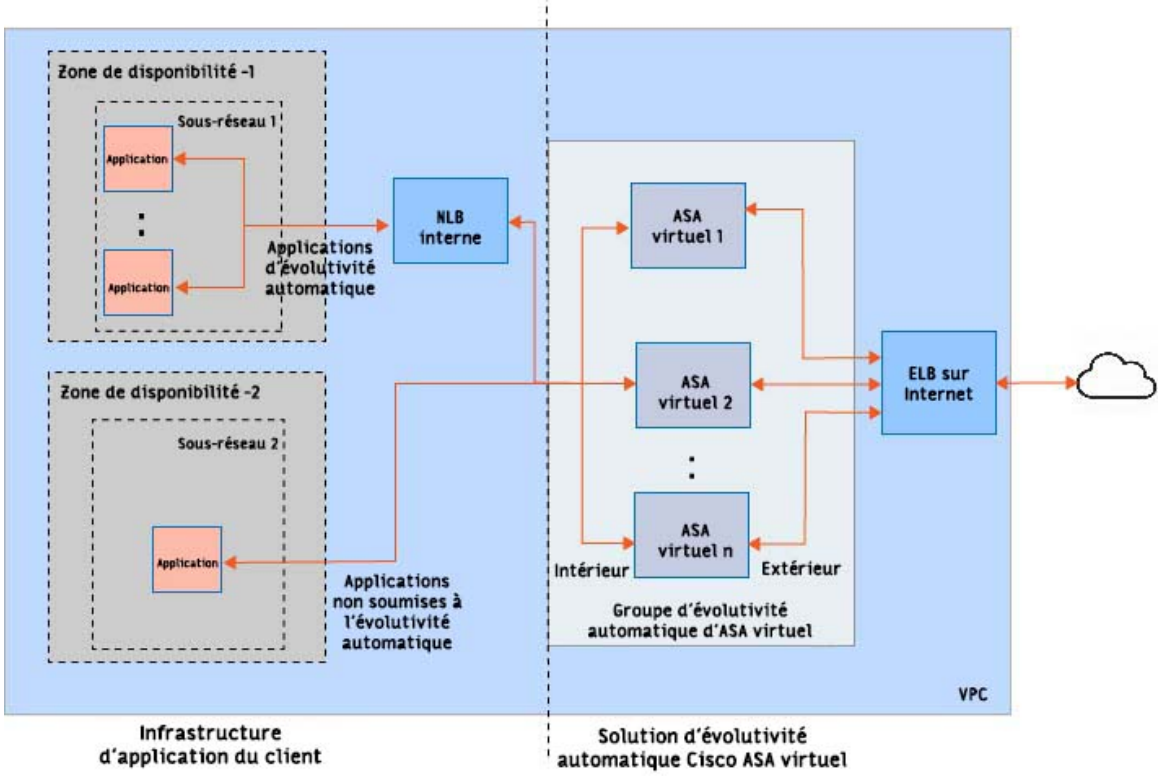
Le scénario de cette solution d'évolutivité automatique AWS ASA virtuel est illustré dans le diagramme des scénarios. Comme l'équilibreur de charges AWS autorise uniquement les connexions entrantes, seul le trafic externe est autorisé à passer à l'intérieur par le pare-feu ASA virtuel.

Remarque Les ports sécurisés ont besoin d'un certificat SSL/TLS, comme décrit dans Certificat de serveur SSL, à la page 108 dans les conditions préalables.

L'équilibreur de charges sur Internet peut être un équilibreur de charges réseau ou un équilibreur de charges d'application. Toutes les exigences et conditions d'AWS sont remplies dans tous les cas. Comme indiqué dans le diagramme des scénarios, le côté droit de la ligne pointillée est déployé par l'intermédiaire des modèles ASA virtuel. Le côté gauche est entièrement défini par l'utilisateur.

Remarque Le trafic sortant initié par l'application ne passera pas par l'ASA virtuel.

Illustration 15 : Diagramme des scénarios d'évolutivité automatique d'ASA virtuel



La bipolation du trafic basée sur le port est possible. Cela peut être possible en utilisant des règles NAT. Par exemple, le trafic DNS LB sur Internet, Port : 80 peut être acheminé vers Application-1; le trafic Port : 88 peut être acheminé vers Application-2.

Fonctionnement de la solution d'évolutivité automatique

Pour l'évolutivité à la baisse et à la hausse des instances ASA virtuel, une entité externe appelée Auto Scale Manager supervise les mesures, les commandes et le groupe d'évolutivité automatique pour ajouter ou supprimer les instances ASA virtuel, et configure les instances ASA virtuel.

Auto Scale Manager est implémenté en utilisant l'architecture sans serveur AWS et communique avec les ressources d'AWS et l'ASA virtuel. Nous fournissons des modèles CloudFormation pour automatiser le déploiement des composants d'Auto Scale Manager. Le modèle déploie également d'autres ressources nécessaires pour que la solution complète fonctionne.

Remarque Les scripts d'évolutivité automatique sans serveur ne sont appelés que par les événements CloudWatch. Ils ne s'exécutent donc que lorsqu'une instance est lancée.

Composants de la solution d'évolutivité automatique

Les composants suivants constituent la solution d'évolutivité automatique.

Modèle CloudFormation

Le modèle CloudFormation est utilisé pour déployer les ressources requises par la solution d'évolutivité automatique dans AWS. Le modèle comprend les éléments suivants :

- Groupe d'évolutivité automatique, équilibreur de charges, groupes de sécurité et autres composants divers.
- Le modèle prend en compte les données des utilisateurs pour personnaliser le déploiement.

Remarque Le modèle a des limites pour la validation des entrées des utilisateurs. Il est donc de la responsabilité de l'utilisateur de valider les entrées pendant le déploiement.

Fonctions Lambda

La solution d'évolutivité automatique est un ensemble de fonctions Lambda développées en Python, qui sont déclenchées à partir de crochets de cycle de vie, de SNS et d'événements/alarmes CloudWatch. Voici les fonctionnalités de base :

- Ajouter/Supprimer les interfaces Gig 0/0 et Gig 0/1 à l'instance.
- Enregistrez l'interface Gig 0/1 dans les groupes cibles de l'équilibreur de charges.
- Configurez et déployez un nouveau ASA virtuel avec le fichier de configuration ASA.

Les fonctions Lambda sont fournies au client sous la forme d'un progiciel Python.

Crochets de cycle de vie

- Les crochets de cycle de vie sont utilisés pour obtenir une notification de modification de cycle de vie d'une instance.
- Dans le cas du lancement d'une instance, un crochet de cycle de vie est utilisé pour déclencher une fonction Lambda qui peut ajouter des interfaces à une instance ASA virtuel et enregistrer les adresses IP d'interface externe aux groupes cibles.
- Dans le cas de la résiliation d'une instance, un crochet de cycle de vie est utilisé pour déclencher une fonction Lambda afin d'annuler l'enregistrement d'une instance ASA virtuel du groupe cible.

Service de notification simple (SNS)

- Le service de notification simple (SNS) d'AWS est utilisé pour générer des événements.
- En raison de la limitation liée à l'absence d'orchestrateur adapté aux fonctions Lambda sans serveur dans AWS, la solution utilise SNS comme type de chaînage de fonctions pour orchestrer les fonctions Lambda selon les événements.

Prérequis

Télécharger les fichiers de déploiement

Téléchargez les fichiers requis pour lancer l'évolutivité automatique d'ASA virtuel pour la solution AWS. Les scripts et les modèles de déploiement pour votre version ASA sont disponibles dans le référentiel GitHub.

Attention Remarque : les scripts et les modèles de déploiement fournis par Cisco pour l'évolutivité automatique sont présentés à titre d'exemples de code source libre et ne font pas l'objet de l'assistance technique du TAC dans sa portée normale. Vérifiez régulièrement GitHub pour connaître les mises à jour et les instructions ReadMe.

Configuration de l'infrastructure

Dans un référentiel GitHub cloné/téléchargé, les fichiers **infrastructure.yaml** se trouvent dans le dossier de modèle. Ce CFT peut être utilisé pour déployer des VPC, des sous-réseaux, des routes, des ACL, des groupes de sécurité, des points terminaux VPC et des compartiments S3 avec des politiques de compartiment. Ce CFT peut être modifié selon vos besoins.

Les sections suivantes fournissent de plus amples renseignements sur ces ressources et leur utilisation dans l'évolutivité automatique. Vous pouvez déployer manuellement ces ressources et les utiliser pour l'évolutivité automatique.

Remarque Le modèle **infrastructure.yaml** déploie uniquement des VPC, des sous-réseaux, des ACL, des groupes de sécurité, des compartiments S3 et des points terminaux de VPC. Il ne crée pas le certificat SSL, la couche Lambda ou les ressources de clés KMS.

VPC

Vous devez créer le VPC selon les besoins de votre application. Il est prévu que le VPC ait une passerelle Internet avec au moins un sous-réseau associé à une route vers Internet. Consultez les sections appropriées pour connaître les exigences des groupes de sécurité, des sous-réseaux, etc.

Subnets (Sous-réseaux)

Des sous-réseaux peuvent être créés selon les besoins de l'application. La machine ASA virtuel nécessite 3 sous-réseaux pour fonctionner, comme illustré dans le scénario.

Remarque Si la prise en charge de plusieurs zones de disponibilité est nécessaire, des sous-réseaux sont nécessaires pour chaque zone, car les sous-réseaux sont des propriétés zonées dans le nuage AWS.

Sous-réseau externe

Le sous-réseau externe doit avoir une route par défaut avec « 0.0.0.0/0 » vers la passerelle Internet. Celui contiendra l'interface externe de l'ASA virtuel, et le NLB sur Internet se trouvera également dans ce sous-réseau.

Sous-réseau interne

Cela peut être similaire aux sous-réseaux d'application, avec ou sans passerelle NAT/Internet. Veuillez noter que pour les sondes d'intégrité de l'ASA virtuel, il devrait être possible d'atteindre le serveur de métadonnées AWS (169.254.169.254) par le port 80.

Remarque Dans cette solution d'évolutivité automatique, les sondes d'intégrité de l'équilibreur de charges sont redirigées vers le serveur de métadonnées AWS par l'intermédiaire de l'interface interne/Gig0/0. Cependant, vous pouvez le modifier en utilisant votre propre application pour assurer les connexions de sonde d'intégrité envoyées à l'ASA virtuel à partir de l'équilibreur de charges. Dans ce cas, vous devez remplacer l'objet du serveur de métadonnées AWS par l'adresse IP de l'application respective pour fournir la réponse des sondes d'intégrité.

Management Subnet (Sous-réseau de gestion)

Ce sous-réseau comprend l'interface de gestion de l'ASA virtuel. Il est facultatif d'avoir une route par défaut.

Sous-réseaux Lambda

La fonction AWS Lambda nécessite deux sous-réseaux ayant la passerelle NAT comme passerelle par défaut. Cela rend la fonction Lambda privée pour le VPC. Les sous-réseaux Lambda ne doivent pas être aussi larges que les autres sous-réseaux. Veuillez vous reporter à la documentation d'AWS pour connaître les bonnes pratiques sur les sous-réseaux Lambda.

Sous-réseaux d'application

Aucune restriction n'est imposée sur ce sous-réseau par la solution d'évolutivité automatique, mais si l'application a besoin de connexions sortantes en dehors du VPC, des routes respectives doivent être configurées

sur le sous-réseau. En effet, le trafic initié vers la sortie ne passe pas par les équilibreurs de charges. Consultez le Guide de l'utilisateur de l'équilibrage de charges élastiques d'AWS.

Groupes de sécurité

Toutes les connexions sont autorisées dans le modèle de groupe d'évolutivité automatique fourni. Vous n'avez besoin que des connexions suivantes pour que la solution d'évolutivité automatique fonctionne.

Tableau 15 : Ports requis

Port	Usage	Sous-réseau
Port de sonde d'intégrité (par défaut : 8080)	Sondes d'intégrité de l'équilibreur de charges sur Internet	Sous-réseaux extérieur, intérieur
Ports d'application	Transit de données des applications	Sous-réseaux extérieur, intérieur

Compartiment Amazon S3

Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de pointe. Vous pouvez placer tous les fichiers requis pour le modèle de pare-feu et le modèle d'application dans le compartiment S3.

Lorsque des modèles sont déployés, des fonctions Lambda sont créées en référençant les fichiers zip dans le compartiment S3. Par conséquent, le compartiment S3 devrait être accessible au compte d'utilisateur.

Certificat de serveur SSL

Si l'équilibreur de charge Internet doit prendre en charge TLS/SSL, un ARN de certificat est requis. Consultez les liens suivants pour en savoir plus :

- Travailler avec des certificats de serveur
- Créer une clé privée et un certificat autosigné pour les tests
- Créer AWS ELB avec un certificat SSL autosigné (lien tiers)

Exemple d'ARN : arn:aws:iam::[Compte AWS]:server-certificate/[Nom du certificat]

Couche Lambda

Le fichier ***autoscale_layer.zip*** peut être créé dans un environnement Linux, comme Ubuntu 18.04 sur lequel Python 3.9 est installé.

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install cffi==1.15.1
pip3 install cryptography==2.9.1
```

```
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
pip3 install pycryptodome==3.15.0
echo "Copy from ./layer directory to ./python\n"
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r autoscale_layer.zip ./python
```

Le fichier ***autoscale_layer.zip*** résultant doit être copié dans le dossier *lambda-python-files*.

Clé principale de KMS

Cela est nécessaire si les mots de passe ASA virtuel sont dans un format chiffré. Sinon, ce composant n'est pas obligatoire. Les mots de passe doivent être chiffrés uniquement à l'aide du KMS fourni ici. Si l'ARN KMS est saisi sur CFT, les mots de passe doivent être chiffrés. Sinon, les mots de passe doivent être en texte brut.

Pour en savoir plus à propos des clés principales et du chiffrement, consultez le document AWS Création de clés et la Référence de commande de l'interface de ligne de commande AWS sur le chiffrement des mots de passe et KMS.

Exemple :

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext 'MyC0mplIc@tedProtect1oN'
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

La valeur de la clé *CiphertextBlob* doit être utilisée comme mot de passe.

Environnement Python 3

Un fichier ***make.py*** se trouve dans le répertoire supérieur du référentiel cloné. Cela compressera les fichiers python dans un fichier zip et les copiera dans un dossier cible. Afin d'effectuer ces tâches, l'environnement Python 3 doit être disponible.

Déployer la solution d'évolutivité automatique

Préparation

Il est attendu que l'application est déployée ou que son plan de déploiement est disponible.

Paramètres d'entrée

Les paramètres d'entrée suivants doivent être recueillis avant le déploiement.

Remarque Pour l'équilibreur de charges de passerelle AWS (GWLB), les paramètres **LoadBalancerType**, **LoadBalancerSG**, **LoadBalancerPort**et **SSLcertificate** ne sont pas applicables.

Tableau 16 : Paramètres d'entrée de l'évolutivité automatique

Paramètre	Valeurs/Type autorisés	Description
PodNumber	Chaîne Modèle autorisé : « ^\d{1,3}$ »	Voici le numéro de module (pod). Ce suffixe sera ajouté au nom du groupe d'évolutivité automatique (ASA virtuel-Nom-Groupe). Par exemple, si cette valeur est « 1 », le nom de groupe sera *ASA virtuel-Nom-Groupe-1*. Il doit comporter au moins 1 chiffre numérique, mais pas plus de 3 chiffres. Par défaut : 1
AutoscaleGrpNamePrefix	Chaîne	Il s'agit du préfixe du nom du groupe d'évolutivité automatique. Le numéro de module (pod) sera ajouté en tant que suffixe. Maximum : 18 caractères Exemple : Cisco-ASA virtuel-1
NotifyEmailID	Chaîne	Les événements de l'évolutivité automatique seront envoyés à cette adresse e-mail. Vous devez accepter une demande d'abonnement par e-mail. Exemple : admin@company.com
VpcId	Chaîne	L'ID du VPC dans lequel l'appareil doit être déployé. Il doit être configuré conformément aux exigences d'AWS. Type : AWS::EC2::VPC::Id Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
LambdaSubnets	Liste	Les sous-réseaux dans lesquels les fonctions Lambda seront déployées. Type : Liste<AWS::EC2::Subnet::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
LambdaSG	Liste	Les groupes de sécurité pour les fonctions Lambda. Type : Liste<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.

Paramètre	Valeurs/Type autorisés	Description
S3BktName	Chaîne	Le nom du compartiment S3 pour les fichiers. Il doit être configuré dans votre compte conformément aux exigences d'AWS. Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
LoadBalancerType	Chaîne	Le type d'équilibreur de charges sur Internet, « application » ou « réseau ». Exemple : application
LoadBalancerSG	Chaîne	Les groupes de sécurité pour l'équilibreur de charges. Dans le cas d'un équilibreur de charges réseau, il ne sera pas utilisé. Mais vous devez fournir un ID de groupe de sécurité. Type : Liste<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
LoadBalancerPort	nombre entier	Le port de l'équilibreur de charges. Ce port sera ouvert sur LB avec le protocole HTTP/HTTPS ou TCP/TLS, en fonction du type d'équilibreur de charges choisi. Assurez-vous que le port est un port TCP valide, il sera utilisé pour créer l'écouteur de l'équilibreur de charges. Par défaut : 80
SSLcertificate	Chaîne	L'ARN du certificat SSL pour les connexions de port sécurisées. S'il n'est pas spécifié, un port ouvert sur l'équilibreur de charges sera TCP/HTTP. S'il est spécifié, un port ouvert sur l'équilibreur de charges sera TLS/HTTPS.
TgHealthPort	Nombre entier	Ce port est utilisé par le groupe cible pour les sondes d'intégrité. Les sondes d'intégrité provenant de ce port sur l'ASA virtuel seront acheminées vers le serveur de métadonnées AWS et ne devraient pas être utilisées pour le trafic. Il doit s'agir d'un port TCP valide. Si vous souhaitez que votre application réponde aux sondes d'intégrité, les règles NAT peuvent être modifiées en conséquence pour l'ASA virtuel. Dans ce cas, si l'application ne répond pas, l'ASA virtuel sera marqué comme non intègre et supprimé en raison de l'alarme de seuil d'instance Non intègre. Exemple : 8080

Paramètre	Valeurs/Type autorisés	Description
AssignPublicIP	Booléen	Si la valeur est sélectionnée comme « true » (vraie), une adresse IP publique sera attribuée. Dans le cas d'un ASA virtuel de type BYOL, vous devez vous connecter à https://tools.cisco.com. Exemple : TRUE (VRAI)
ASAvInstanceType	Chaîne	L'Amazon Machine Image (AMI) prend en charge différents types d'instances, qui déterminent la taille de l'instance et la quantité de mémoire requise. Seuls les types d'instances AMI qui prennent en charge l'ASA virtuel doivent être utilisés. Exemple : c4.2xlarge
ASAvLicenseType	Chaîne	Le type de licence ASA virtuel, BYOL ou PAYG. Assurez-vous que l'ID AMI associé est du même type de licence. Exemple : BYOL
ASAvAmiId	Chaîne	L'ID AMI d'ASA virtuel (un ID AMI de Cisco ASA virtuel valide). Type : AWS::EC2::Image::Id Veuillez choisir le bon ID AMI en fonction de la région et de la version souhaitée de l'image.
ConfigFileURL	Chaîne	L'URL HTTP pour les fichiers de configuration d'ASA virtuel. Les fichiers de configuration de chaque zone de disponibilité doivent être disponibles dans l'URL. La fonction Lambda se chargera de choisir le bon fichier. Vous pouvez déployer un serveur HTTP pour héberger des fichiers de configuration ou vous pouvez utiliser la fonction d'hébergement web statique d'AWS S3. **Remarque** Le dernier « / » est également nécessaire, car les noms des fichiers de configuration seront ajoutés à l'URL au moment de l'importation. Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur. Exemple : https://myserver/asavconfig/asaconfig .txt/

Paramètre	Valeurs/Type autorisés	Description
NoOfAZs	Nombre entier	Le nombre de zones de disponibilité que l'ASA virtuel doit traverser, entre 1 et 3. Dans le cas d'un déploiement ALB, la valeur minimale est de 2, comme l'exige AWS. Exemple : 2
ListOfAzs	Chaîne séparée par des virgules	Une liste de zones séparées par des virgules dans l'ordre. **Remarque** L'ordre dans lequel elles sont énumérées est important. Les listes de sous-réseaux doivent être données dans le même ordre. Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur. Exemple : us-east-1a, us-east-1b, us-east-1c
ASAvMgmtSubnetId	Liste séparée par des virgules	Une liste d'ID de sous-réseau de gestion séparés par des virgules. La liste doit être dans le même ordre que les zones de disponibilité correspondantes. Type : Liste<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
ASAvInsideSubnetId	Liste séparée par des virgules	Une liste d'ID de sous-réseau interne/Gig0/0 séparés par des virgules. La liste doit être dans le même ordre que les zones de disponibilité correspondantes. Type : Liste<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.
ASAvOutsideSubnetId	Liste séparée par des virgules	Une liste d'ID de sous-réseau externe/Gig0/1 séparés par des virgules. La liste doit être dans le même ordre que les zones de disponibilité correspondantes. Type : Liste<AWS::EC2::SecurityGroup::Id> Si le fichier « *infrastructure.yaml* » est utilisé pour déployer l'infrastructure, la section de sortie de la pile aura cette valeur. Veuillez utiliser cette valeur.

Paramètre	Valeurs/Type autorisés	Description
KmsArn	Chaîne	L'ARN d'un KMS existant (clé AWS KMS à chiffrer au repos). S'ils sont spécifiés, les mots de passe ASA virtuel doivent être chiffrés. Le chiffrement du mot de passe doit être effectué uniquement à l'aide de l'ARN spécifié. Exemple de génération de mot de passe chiffré : « aws kms encrypt --key-id <ARN KMS> --plaintext <password> ». Veuillez utiliser les mots de passe générés, comme indiqué. Exemple : arn:aws:kms:us-east-1:[Compte AWS]:key/7d586a25-5875-43b1-bb68-a452e2f6468e
CpuThresholds	Nombre entiers séparés par des virgules	Le seuil inférieur et le seuil supérieur pour le CPU. La valeur minimale est de 0 et la valeur maximale est de 99. Par défaut : 10, 70 Veuillez noter que le seuil inférieur doit être inférieur au seuil supérieur. Exemple : 30, 70

Mettre à jour les fichiers de configuration ASA

Vous préparez des fichiers de configuration ASA et vous les stockez dans un serveur http/https accessible par une instance ASA virtuel. Il s'agit d'un format de fichier de configuration ASA standard. Un ASA virtuel évolutif téléchargera un fichier de configuration et mettra à jour sa configuration.

Les sections suivantes fournissent des exemples sur la façon dont le fichier de configuration ASA peut être modifié pour la solution d'évolutivité automatique.

Objets, groupes de périphériques, règles NAT et politiques d'accès

Consultez les éléments suivants pour obtenir un exemple d'objets, de routes et de règles NAT pour les sondes d'intégrité de l'équilibreur de charges pour la configuration ASA virtuel.

```
! Load Balancer Health probe Configuration
object network aws-metadata-server
host 169.254.169.254
object service aws-health-port
service tcp destination eq 7777
object service aws-metadata-http-port
service tcp destination eq 80
route inside 169.254.169.254 255.255.255.255 10.0.100.1 1
nat (outside,inside) source static any interface destination static interface
aws-metadata-server service aws-health-port aws-metadata-http-port
!
```

Remarque Les connexions de sonde d'intégrité ci-dessus doivent être autorisées dans votre politique d'accès.

Consultez la section suivante pour obtenir un exemple de configuration du plan de données pour une configuration ASA virtuel.

```
! Data Plane Configuration
route inside 10.0.0.0 255.255.0.0 10.0.100.1 1
object network http-server-80
host 10.0.50.40
object network file-server-8000
host 10.0.51.27
object service http-server-80-port
service tcp destination eq 80
nat (outside,inside) source static any interface destination static interface http-server-80
 service http-server-80-port http-server-80-port
object service file-server-8000-port
service tcp destination eq 8000
nat (outside,inside) source static any interface destination static interface file-server-8000
 service file-server-8000-port file-server-8000-port
object service https-server-443-port
service tcp destination eq 443
nat (outside,inside) source static any interface destination static interface http-server-80
 service https-server-443-port http-server-80-port
!
```

Mises à jour des fichiers de configuration

La configuration ASA virtuel doit être mise à jour dans les fichiers *az1-configuration.txt*, *az2-configuration.txt*et *az3-configuration.txt*.

Remarque Avoir trois fichiers de configuration vous permet de modifier la configuration en fonction de la zone de disponibilité (AZ). Par exemple, la route statique vers le serveur aws- metadata-server aura une passerelle différente dans chaque zone de disponibilité.

Mises à jour du modèle

Le modèle *deploy_autoscale.yaml* doit être modifié avec soin. Vous devez modifier le champ *UserData* (données utilisateur) du ***LaunchTemplate*** (modèle de lancement). Le champ *UserData* (données utilisateur) peut être mis à jour au besoin. Le serveur de noms *name-server* doit être mis à jour en conséquence; par exemple, il peut s'agir de l'adresse IP DNS du VPC. Lorsque votre licence est BYOL, l'*idtoken* (jeton d'identité) de licence doit être partagé ici.

```
!
dns domain-lookup management
DNS server-group DefaultDNS
name-server <VPC DNS IP>
!
! License configuration
        call-home
        profile License
        destination transport-method http
        destination address http <url>
        license smart
        feature tier standard
        throughput level <entitlement>
        license smart register idtoken <token>
```

Charger des fichiers dans le service de stockage Amazon Simple Storage (S3)

Tous les fichiers du répertoire *cible* doivent être chargés dans le compartiment Amazon S3. Vous pouvez également utiliser l'interface de ligne de commande pour charger tous les fichiers du répertoire *cible* dans le compartiment Amazon S3.

```
$ cd ./target
$ aws s3 cp . s3://<bucket-name> --recursive
```

Déployer la pile

Une fois que toutes les conditions préalables pour le déploiement sont terminées, vous pouvez créer la pile AWS CloudFormation.

Utilisez le fichier *deploy_autoscale.yaml* dans le répertoire *target* (cible).

Utilisez le fichier *deploy_ngfw_autoscale_with_gwlb.yaml* dans le répertoire *target* (cible) pour Geneve Autoscale.

Remarque Avant de déployer le fichier *deploy_ngfw_autoscale_with_gwlb.yaml* , vous devez déployer le fichier **infrastructure_gwlb.yaml** pour la solution d'évolutivité automatique AWS GWLB.

Vous devez créer le point terminal de l'équilibreur de charge de passerelle (GWLB-E) en sélectionnant le GWLB qui est créée lors du déploiement du modèle *deploy_autoscale_with_gwlb.Yaml*. Après avoir créé le GWLBe, vous devez mettre à jour le routeur par défaut pour utiliser GWLBe pour le sous-réseau d'application et le tableau de routage par défaut.

Pour en savoir plus, consultez https://docs.amazonaws.cn/en_us/vpc/latest/privatelink/create-endpoint-service-gwlbe.html.

Fournissez les paramètres comme collectés dans Paramètres d'entrée, à la page 109.

Valider les déploiements

Une fois le déploiement du modèle réussi, vous devez valider que les fonctions Lambda et les événements CloudWatch sont créés. Par défaut, le groupe d'évolutivité automatique a le nombre minimal et maximal d'instances à zéro. Vous devez modifier le groupe d'évolutivité automatique dans la console AWS EC2 avec le nombre d'instances que vous souhaitez. Cela déclenchera les nouvelles instances ASA virtuel.

Nous vous recommandons de lancer une seule instance, de vérifier son flux de travail et de valider son comportement pour savoir si elle fonctionne comme prévu. Une fois que les exigences réelles de l'ASA virtuel peuvent être déployées, elle peuvent également vérifier le comportement. Le nombre minimal d'instances ASA virtuel peut être marqué comme protégé contre une évolutivité à la baisse pour éviter que ces dernières soient supprimées par les politiques d'évolutivité AWS.

Tâches de maintenance

Processus d'évolutivité

Cette rubrique explique comment suspendre puis reprendre un ou plusieurs des processus d'évolutivité pour votre groupe d'évolutivité automatique.

Actions de début et de fin d'évolutivité

Pour commencer et arrêter les actions d'évolutivité à la hausse/baisse, procédez comme suit.

- Pour l'évolutivité dynamique d'AWS, consultez le lien suivant pour obtenir des renseignements afin d'activer ou de désactiver les actions d'évolutivité à la hausse :

  Suspension et reprise des processus d'évolutivité

Moniteur d'intégrité

Toutes les 60 minutes, une tâche CloudWatch Cron déclenche le gestionnaire d'évolutivité automatique Lambda pour le module d'intégrité :

- S'il y a des adresses IP non intègres qui appartiennent à une machine virtuelle ASA virtuel valide, cette instance est supprimée si l'ASA virtuel date de plus d'une heure.
- Si ces adresses IP ne proviennent pas d'une machine ASA virtuel valide, seules les adresses IP sont supprimées du groupe cible.

Désactiver le moniteur d'intégrité

Pour désactiver un moniteur d'intégrité, dans ***constant.py***, définissez la constante sur « True » (Vrai).

Activer le moniteur d'intégrité

Pour activer un moniteur d'intégrité, dans ***constant.py***, définissez la constante sur « False » (Faux).

Désactiver les crochets de cycle de vie

Dans le cas peu probable où le crochet de cycle de vie doit être désactivé, s'il est désactivé, il n'ajoutera pas d'interfaces supplémentaires aux instances. Cela peut également entraîner une série d'échecs du déploiement des instances ASA virtuel.

Désactiver le gestionnaire d'évolutivité automatique

Pour désactiver le gestionnaire d'évolutivité automatique, les événements CloudWatch « notify-instance-launch » et « notify-instance-terminate » doivent être désactivés. Cette désactivation ne déclenchera pas Lambda pour de nouveaux événements. Mais l'exécution des actions Lambda se poursuivra déjà. Il n'y a pas d'arrêt brutal du gestionnaire d'évolutivité automatique. La tentative d'arrêt brut par la suppression de la pile ou la suppression des ressources peut entraîner un état indéfini.

Cibles de l'équilibreur de charge

Comme l'équilibreur de charge AWS n'autorise pas les cibles de type instance pour les instances ayant plusieurs interfaces réseau, l'adresse IP de l'interface Gigabit0/1 est configurée comme cible sur les groupes de cibles. Pour l'instant, cependant, les contrôles d'intégrité de l'évolutivité automatique d'AWS ne fonctionnent que pour les cibles de type d'instance, et non pour les adresses IP. En outre, ces adresses IP ne sont pas automatiquement ajoutées ou supprimées des groupes cibles. Par conséquent, notre solution d'évolutivité automatique gère ces deux tâches de manière programmatique. Mais dans le cas d'une maintenance ou d'un dépannage, il pourrait y avoir une situation nécessitant un effort manuel.

Enregistrer une cible dans un groupe de cibles

Pour enregistrer l'instance ASA virtuel sur l'équilibreur de charge, son adresse IP d'instance Gigabit0/1 (sous-réseau externe) doit être ajoutée en tant que cible dans le ou les groupes de cibles. Consultez Enregistrer ou annuler l'enregistrement des cibles par adresse IP.

Annuler l'enregistrement d'une cible d'un groupe de cibles

Pour annuler l'enregistrement de l'instance ASA virtuel de l'équilibreur de charge, son adresse IP d'instance Gigabit0/1 (sous-réseau externe) doit être supprimée en tant que cible dans le ou les groupes de cibles. Consultez Enregistrer ou annuler l'enregistrement des cibles par adresse IP.

Instance en veille

AWS n'autorise pas le redémarrage d'instance dans le groupe d'évolutivité automatique, mais il permet à un utilisateur de mettre une instance en veille et d'effectuer de telles actions. Cependant, cela fonctionne mieux lorsque les cibles de l'équilibreur de charges sont de type instance. Cependant, les machines ASA virtuel ne peuvent pas être configurées en tant que cibles de type instance, en raison de plusieurs interfaces réseau.

Mettre une instance en veille

Si une instance est mise en veille, son adresse IP dans les groupes de cibles continuera toujours d'être dans le même état jusqu'à ce que les sondes d'intégrité échouent. Pour cette raison, il est recommandé de désinscrire les adresses IP respectives du groupe cible avant de mettre l'instance en état de veille; consultez Annuler l'enregistrement d'une cible d'un groupe de cibles, à la page 118 pour en savoir plus.

Une fois les IP supprimées, consultez Supprimer temporairement les instances de votre groupe d'évolutivité automatique.

Supprimer une instance de la mise en veille

De même, vous pouvez déplacer une instance de l'état de veille à l'état d'exécution. Après sa suppression de l'état de veille, l'adresse IP de l'instance doit être enregistrée sur les cibles du groupe cible. Consultez Enregistrer une cible dans un groupe de cibles, à la page 118.

Pour en savoir plus sur la mise en veille des instances à des fins de dépannage ou de maintenance, consultez le blogue d'actualités AWS.

Supprimer/dissocier l'instance du groupe d'évolutivité automatique

Pour supprimer une instance du groupe d'évolutivité automatique, vous devez d'abord la mettre en mode veille. Consultez la section « Mettre des instances en veille ». Une fois que l'instance est en état de veille, elle

peut être supprimée ou dissociée. Consultez Dissocier les instances EC2 de votre groupe d'évolutivité automatique.

Mettre fin à une instance

Pour mettre fin à une instance, elle doit être mise en veille; voir Instance en veille, à la page 118. Une fois que l'instance est en veille, vous pouvez procéder à la résiliation.

Protection de l'instance par l'évolutivité à la baisse

Pour éviter la suppression accidentelle d'une instance particulière du groupe d'évolutivité automatique, elle peut être protégée par l'évolutivité à la baisse. Si une instance est protégée par l'évolutivité à la baisse, elle ne sera pas résiliée en raison d'un événement d'évolutivité à la baisse.

Veuillez vous reporter au lien suivant pour mettre une instance en état protégé par l'évolutivité à la baisse.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

Important Il est recommandé de faire en sorte que le nombre minimal d'instances qui sont intègres (l'adresse IP cible doit être intègre, pas seulement l'instance EC2) soit protégé par l'évolutivité à la baisse.

Changements de configuration

Toute modification de la configuration ne sera pas automatiquement reflétée sur les instances déjà en cours d'exécution. Ces modifications ne seront reflétées que sur les prochains périphériques intégrés. Toutes les modifications de ce type doivent être transférées manuellement vers les périphériques existants.

Si vous rencontrez des problèmes lors de la mise à jour manuelle de la configuration sur les instances existantes, nous vous recommandons de supprimer ces instances du groupe d'évolutivité et de les remplacer par de nouvelles.

Modifier le mot de passe d'administrateur ASA virtuel

Une modification du mot de passe ASA virtuel oblige l'utilisateur à le modifier sur chaque périphérique manuellement pour les instances en cours d'exécution. Pour les nouveaux périphériques ASA virtuel à intégrer, le mot de passe ASA virtuel sera tiré des variables d'environnement Lambda. Consultez la section Utilisation des variables d'environnement AWS Lambda.

Modifications des ressources AWS

Vous pouvez modifier de nombreuses choses dans AWS après le déploiement, telles que le groupe d'évolutivité automatique, la configuration de lancement, les événements CloudWatch, les politiques d'évolutivité, etc. Vous pouvez importer vos ressources dans une pile CloudFormation ou créer une nouvelle pile à partir de vos ressources existantes.

Consultez la section Importation de ressources existantes dans CloudFormation Management pour en savoir plus sur la gestion des modifications effectuées sur les ressources d'AWS.

Récupérer et analyser les journaux CloudWatch

Afin d'exporter les journaux CloudWatch, consultez la section Exporter les données du journal vers Amazon S3 à l'aide de l'interface de ligne de commande d'AWS.

Dépannage et débogage

Console AWS CloudFormation

Vous pouvez vérifier les paramètres d'entrée de votre pile CloudFormation dans la console AWS CloudFormation, qui vous permet de créer, de superviser, de mettre à jour et de supprimer des piles directement à partir de votre navigateur Web.

Accédez à la pile requise et vérifiez l'onglet des paramètres. Vous pouvez également vérifier les entrées des fonctions Lambda sous l'onglet des variables d'environnement des fonctions Lambda.

Pour en savoir plus sur la console AWS CloudFormation, consultez le *Guide de l'utilisateur AWS CloudFormation*.

Journaux Amazon CloudWatch

Vous pouvez afficher les journaux des fonctions Lambda individuelles. AWS Lambda supervise automatiquement les fonctions Lambda en votre nom, en effectuant des rapports sur les mesures par l'entremise d'Amazon CloudWatch. Pour vous aider à dépanner les défaillances d'une fonction, Lambda consigne toutes les demandes gérées par votre fonction et stocke également automatiquement les journaux générés par votre code dans les journaux Amazon CloudWatch.

Vous pouvez afficher les journaux pour Lambda en utilisant la console Lambda, la console CloudWatch, l'interface CLI 'AWS ou l'API CloudWatch. Pour en savoir plus sur les groupes de journaux et y accéder par l'entremise de la console CloudWatch, consultez le système de supervision, l'application et les fichiers journaux personnalisés dans le *Guide de l'utilisateur Amazon CloudWatch*.

Échec de contrôle de l'intégrité de l'équilibreur de charges

Le contrôle de l'intégrité de l'équilibreur de charges contient des informations telles que le protocole, le port ping, le chemin ping, le délai d'expiration de réponse et l'intervalle de contrôle de l'intégrité. Une instance est considérée comme saine si elle renvoie un code de réponse de 200 dans l'intervalle de contrôle de l'intégrité.

Si l'état actuel de certaines ou de toutes vos instances est `Outofservice` et que le champ de description affiche le message que `Instance has failed at least the Unhealthy Threshold number of health checks consecutively` (l'instance a échoué au moins à un nombre limite de contrôles d'intégrité consécutifs), les instances ont échoué au contrôle de l'intégrité de l'équilibreur de charges.

Vous devez vérifier la règle NAT de la sonde d'intégrité dans la configuration ASA. Pour en savoir plus, consultez Dépannage d'un équilibreur de charges classique : contrôles d'intégrité.

Problèmes de trafic

Pour résoudre les problèmes de trafic pour vos instances ASA virtuel, vous devez vérifier les règles de l'équilibreur de charge, les règles NAT et les routes statiques configurées dans les instances ASA virtuel.

Vous devez également vérifier les détails du réseau virtuel AWS, des sous-réseaux et de la passerelle fournis dans le modèle de déploiement, y compris les règles de groupe de sécurité, etc. Vous pouvez également consulter la documentation AWS, par exemple, Dépannage des instances EC2.

Échec de la configuration de ASA virtuel

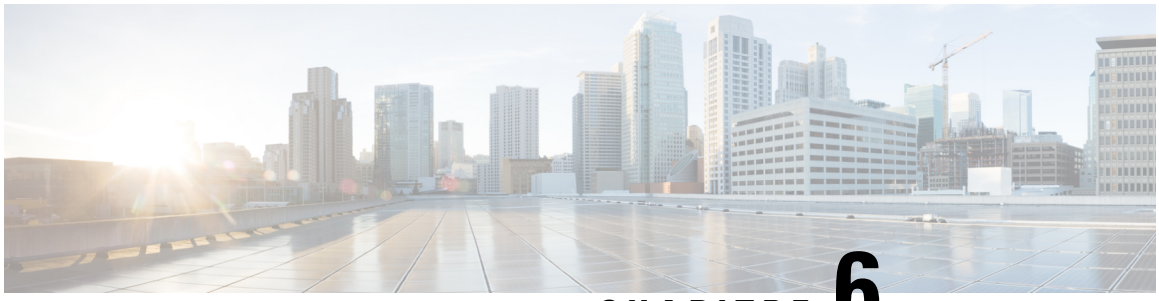
Si l'ASA virtuel ne parvient pas à se configurer, vous devez vérifier la connectivité à la configuration d'hébergement du serveur Web HTTP statique Amazon S3. Consultez Hébergement d'un site Web statique sur Amazon S3 pour en savoir plus.

Échec de la licence ASA virtuel

Si la licence ASA virtuel échoue, vous devez vérifier la connectivité au serveur CSSM, vérifiez la configuration du groupe de sécurité ASA virtuel et vérifiez les listes de contrôle d'accès.

Impossible d'inscrire le protocole SSH dans l'ASA virtuel

Si vous ne parvenez pas à inscrire le protocole SSH dans l'ASA virtuel, vérifiez si le mot de passe complexe a été transmis à l'ASA virtuel au moyen du modèle.



CHAPITRE 6

Déployer l'ASA virtuel sur Microsoft Azure Cloud

Vous pouvez déployer l'ASA virtuel sur le nuage Microsoft Azure.

Important À partir de la version 9.13(1), toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge. Cela permet aux ASA virtuel clients de fonctionner sur une grande variété de profils de ressources VM. Cela augmente également le nombre d'instances Azure prises en charge.

- Aperçu, à la page 123
- Prérequis, à la page 125
- Lignes directrices et limites relatives à la licence, à la page 126
- Ressources créées lors du déploiement, à la page 129
- Routage Azure, à la page 130
- Configuration du routeur pour les machines virtuelles dans le réseau virtuel, à la page 130
- Adresses IP, à la page 131
- DNS, à la page 131
- Mise en réseau accélérée (AN), à la page 132
- Déployer l'ASA virtuel, à la page 132
- Annexe : Exemple de modèle de ressource Azure, à la page 142

Aperçu

Sélectionnez le niveau et la taille de machine virtuelle Azure qui répondent à vos besoins ASA virtuel. Toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuelprise en charge. Cela vous permet d'exécuter l'ASA virtuel sur une grande variété de types d'instances Azure.

Tableau 17 : Types d'instances pris en charge par Azure

Instance	Attributs		Interfaces
	vCPU	Mémoire (Go)	
D3, D3_v2, DS3, DS3_v2	4	14	4
D4, D4_v2, DS4, DS4_v2	8	28	8

Instance	Attributs		Interfaces
	vCPU	Mémoire (Go)	
D5, D5_v2, DS5, DS5_v2	16	56	8
D8_v3	8	32	4
D16_v3	16	64	4
D8s_v3	8	32	4
D16s_v3	16	64	8
F4, F4s	4	8	4
F8, F8s	8	16	8
F16, F16s	16	32	8
F8s_v2	8	16	4
F16s_v2	16	32	8

Tableau 18 : ASA virtuel Limites des fonctionnalités sous licence en fonction des droits

Niveau de performance	Type d'instance (cœur/RAM)	Limite du débit	Limite de session RA VPN
ASAv5	D3_v2 4 cœurs/14 Go	100 Mbit/sec	50
ASAv10	D3_v2 4 cœurs/14 Go	1 Gbit/sec	250
ASAv30	D3_v2 4 cœurs/14 Go	2 Gbit/s	750
ASAv50	D4_v2 8 cœurs/28 Go	5,5 Gbit/s	10 000
ASAv100	D5_v2 16 cœurs/56 Go	11 Gbit/s	20 000

Vous pouvez déployer l'ASA virtuel sur Microsoft Azure :

- En tant que pare-feu autonome à l'aide d'Azure Resouce Manager sur le nuage public Azure standard et les environnements Azure pour le gouvernement
- En tant que solution partenaire intégrée à l'aide d'Azure Security Center
- En tant que paire à haute accessibilité à l'aide d'Azure Resource Manager sur le nuage public Azure standard et les environnements Azure pour le gouvernement.

Consultez Déployer l'ASA virtuel à partir d'Azure Resource Manager, à la page 133. Notez que vous pouvez déployer la configuration ASA virtuel à haute disponibilité sur le nuage public Azure standard et les environnements Azure pour le gouvernement.

Prérequis

- Créez un compte sur Azure.com.

  Après avoir créé un compte sur Microsoft Azure, vous pouvez vous connecter, choisir l'ASA virtuel dans le Marché Microsoft Azure et déployer l'ASA virtuel.

- Obtenez une licence pour l'ASA virtuel.

  Jusqu'à ce que vous obteniez une licence pour l'ASA virtuel, il fonctionnera en mode dégradé, ce qui n'autorisera que 100 connexions et un débit de 100 kbit/s. Consultez Obtention des licences logicielles Smart pour l'ASA virtuel.

Remarque L'ASA virtuel prend la valeur par défaut du droit à 2 Gbit/s lorsqu'il est déployé sur Azure. L'utilisation du droit à 100 Mbit/s et 1 Gbit/s est autorisée. Cependant, le niveau de débit doit être configuré explicitement pour utiliser le droit à 100 Mbit/s ou à 1 Gbit/s.

- Exigences d'interface :

  Vous devez déployer l'ASA virtuel avec quatre interfaces sur quatre réseaux. Vous pouvez attribuer une adresse IP publique à n'importe quelle interface. consultez Adresses IP publiques pour connaître les lignes directries d'Azure concernant les adresses IP publiques, y compris comment créer, modifier ou supprimer une adresse IP publique.

- Interface de gestion :

  Dans Azure, la première interface définie est toujours l'interface de gestion.

- Chemins de communication :

  - Interface de gestion : utilisée pour l'accès SSH et pour connecter l'ASA virtuel à l'ASDM.

Remarque La mise en réseau accélérée Azure n'est pas prise en charge sur l'interface de gestion.

  - Interface interne (requise) : utilisée pour connecter l'ASA virtuel aux hôtes internes.
  - Interface externe (requise) : utilisée pour connecter l'ASA virtuel au réseau public.
  - Interface DMZ (facultative) : utilisée pour connecter l'ASA virtuel au réseau DMZ lors de l'utilisation de l'interface Standard_D3.

- Pour en savoir plus sur l'hyperviseur ASA virtuel et la plateforme virtuelle, consultez compatibilité de Cisco Cisco Secure Firewall ASA.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

- Déploiement à partir de Microsoft Azure Cloud
- Mise en réseau accélérée (AN) Azure
- Maximum de 16 vCPU, en fonction du type d'instance sélectionné

Remarque Azure ne fournit pas de capacité vSwitch configurable de couche 2.

- Adresse IP publique sur n'importe quelle interface

  Vous pouvez attribuer une adresse IP publique à n'importe quelle interface; consultez Adresses IP publiques pour connaître les lignes directrices d'Azure concernant les adresses IP publiques, y compris comment créer, modifier ou supprimer une adresse IP publique.

- Mode de pare-feu routé (par défaut)

Remarque En mode de pare-feu routé, l'ASA virtuel est une limite traditionnelle de couche 3 dans le réseau. Ce mode requiert une adresse IP pour chaque interface. Comme Azure ne prend pas en charge les interfaces balisées VLAN, les adresses IP doivent être configurées sur les interfaces non balisées et sans liaison.

Fonctionnalité Azure DDoS Protection

Azure DDoS Protection dans Microsoft Azure est une fonctionnalité supplémentaire implémentée à l'avant d'ASA virtuel. Dans un réseau virtuel, lorsque cette fonctionnalité est activée, elle aide à défendre les applications contre les attaques courantes de couche de réseau en fonction du paquet par seconde du trafic attendu d'un réseau. Vous pouvez personnaliser cette fonctionnalité en fonction du modèle de trafic réseau.

Pour en savoir plus sur la fonctionnalité Azure DDoS Protection, consultez Présentation de la norme Azure DDoS Protection.

Configuration du mot de passe

Assurez-vous que le mot de passe que vous définissez est conforme aux lignes directrices indiquées ci-dessous. Le mot de passe doit :

- être une chaîne alphanumérique avec un minimum de 12 caractères et un maximum de 72 caractères
- être composé de caractères minuscules et majuscules, de chiffres et de caractères spéciaux qui ne sont pas « \ » ou « - »
- ne pas comporter plus de 2 caractères ASCII répétés ou séquentiels
- ne pas être un mot que l'on peut trouver dans le dictionnaire

Si vous observez des problèmes de déploiement, tels que ceux énumérés ci-dessous, ou d'autres erreurs liées au mot de passe dans les journaux de démarrage, vous devez vérifier si votre mot de passe configuré est conforme aux lignes directrices en matière de complexité de mots de passe.

Erreurs de déploiement

- `OS Provisioning failed for VM 'TEST-CISCO-TDV-QC' due to an internal error. (Code: OSProvisioningInternal Error)`

- ```
  OS Provisioning failed for VM 'TEST-CISCO-ASAVM' due to an internal error.
  InternalDetail: RoleInstanceContainerProvisioningDetails:
  MediaStorageAccountName:ProvisionVmWithUpdate; MediaStorageHostName:ProvisionVmWithUpdate;
   MediaRelativeUrl:ProvisionVmWithUpdate;
  MediaTenantSecretId:00000000-0000-0000-0000-000000000000; ProvisioningResult:Failure;
  ProvisioningResultMessage:[ProtocolError] [CopyOvfEnv]
  Error mounting dvd: [OSUtilError] Failed to mount dvd device Inner error: [mount -o ro
   -t udf,iso9660 /dev/hdc /mnt/cdrom/secure] returned 32:
  mount: /mnt/cdrom/secure: no medium found on /dev/hdc
  ```

Vous pouvez examiner et reconfirmer ces erreurs liées au mot de passe en vous référant au journal de la console de série. Voici un exemple de détail d'erreur provenant d'un journal de console de série :

```
10150 bytes copied in 0.80 secs
Waagent - 2024-08-02T00:46:55.889400Z INFO Daemon Create user account if not exists
Waagent - 2024-08-02100:46:55.890685Z INFO Daemon Set user password.
ERROR: Password must contain:
ERROR: a value that has less than 3 repetitive or sequential ASCII characters.
Invalid Eg:aaaauser, user4321, aaabc789
Failed to add username "cisco"
ADD_USER reply indicates failure
```

Problèmes connus

Délai d'inactivité

L'ASA virtuel sur Azure a un *délai d'inactivité* configurable sur la VM. Le paramètre minimal est de 4 minutes et le paramètre maximal est de 30 minutes. Cependant, pour les sessions SSH, le paramètre minimal est de 5 minutes et le paramètre maximal est de 60 minutes.

Remarque Sachez que le délai d'inactivité de l'ASA virtuelremplace toujours le délai d'expiration SSH et déconnecte la session. Vous pouvez choisir de faire correspondre le délai d'inactivité de la VM au délai d'expiration SSH afin que la session n'expire pas de chaque côté.

Basculement de l'ASA virtuel principal à l'ASA virtuel de secours

Lorsqu'une mise à niveau Azure se produit sur un ASA virtuel haute disponibilité dans le déploiement Azure, un basculement peut se produire de l'ASA virtuel principal à l'ASA virtuelde secours. Une mise à niveau Azure fait entrer l'ASA virtuel principal dans un état de pause. L'ASA virtuel de secours ne reçoit pas de paquets Hello lorsque l'ASA virtuel principal est en pause. Si l'ASA virtuel de secours ne reçoit pas de paquets Hello au-delà du délai de rétention du basculement, un basculement vers l'ASA virtuel de secours se produit.

Il est également possible qu'un basculement se produise même si le délai de rétention du basculement n'a pas été dépassé. Imaginez un scénario dans lequel l'ASA virtuel principal reprend 19 secondes après être passé à l'état de pause. Le délai de rétention du basculement est de 30 secondes. Mais, l'ASA virtuel de secours ne reçoit pas les paquets Hello avec l'horodatage approprié, car l'horloge est synchronisée toutes les ~2 minutes. Cela entraîne un basculement de l'ASA virtuel principal vers l'ASA virtuelde secours.
```

Remarque Cette fonctionnalité prend uniquement en charge IPv4. L'ASA virtuel haute disponibilité n'est pas pris en charge pour la configuration IPv6.

Fonctionnalités non prises en charge

- Accès à la console (la gestion est effectuée à l'aide de SSH ou ASDM sur les interfaces réseau)
- Balisage du VLAN sur les interfaces d'instance d'utilisateur
- Bâtis grand format
- ARP de mandataire pour une adresse IP que l'appareil ne possède pas du point de vue d'Azure
- Mode promiscuité (pas de prise en charge du pare-feu en mode sniffer (analyseur réseau) ou transparent)

Remarque La politique Azure empêche l'ASA virtuel de fonctionner en mode de pare-feu transparent, car elle n'autorise pas les interfaces à fonctionner en mode promiscuité.

- Mode multi-contexte
- Mise en grappes
- ASA virtuel natif à haute disponibilité

Remarque Vous pouvez déployer l'ASA virtuel sur Azure dans une configuration active/de secours à haute disponibilité (HA) sans état.

- Importation/exportation de VM
- Par défaut, le mode FIPS n'est pas activé sur l'ASA virtuel exécuté dans le nuage Azure.

Remarque Si vous activez le mode FIPS, vous devez remplacer le groupe d'échange de clés Diffie-Helman par une clé plus renforcée à l'aide de la commande **ssh key-exchange group dh-group14-sha1**. Si vous ne modifiez pas le groupe Diffie-Helman, vous ne pourrez plus vous connecter à SSH avec l'ASA virtuel, et c'est la seule façon de gérer initialement l' ASA virtuel.

- IPv6
- Génération de VM de 2e génération sur Azure
- Redimensionner la VM après le déploiement
- Migration ou mise à jour de l'UGS de stockage Azure pour le disque du système d'exploitation de la VM de l'UGS premium à l'UGS standard et inversement

Ressources créées lors du déploiement

Lorsque vous déployez l'ASA virtuel dans Azure, les ressources suivantes sont créées :

- La machine ASA virtuel
- Un groupe de ressources (sauf si vous avez choisi un groupe de ressources existant)

  Le groupe de ressources ASA virtuel doit être le même groupe de ressources utilisé par le réseau virtuel et le compte de stockage.
- Quatre NIC nommés nom vm-Nic0, nom vm-Nic1, nom vm-Nic2, nom vm-Nic3

  Ces cartes réseau (NIC) correspondent aux interfaces ASA virtuel Management 0/0, GigabitEthernet 0/0, GigabitEthernet 0/1 et GigabitEthernet 0/2, respectivement.

Remarque Selon les besoins, vous pouvez créer un réseau virtuel avec IPv4 uniquement .

- Un groupe de sécurité nommé nom vm-SSH-SecurityGroup

  Le groupe de sécurité sera associé à la Nic0 de la machine virtuelle, qui correspond à ASA virtuel Management 0/0.

  Le groupe de sécurité comprend des règles qui autorisent le protocole SSH, et les ports UDP 500 et UDP 4500 à des fins de réseau privé virtuel (VPN). Vous pourrez modifier ces valeurs après le déploiement.
- Adresses IP publiques (nommées en fonction de la valeur que vous avez choisie lors du déploiement)

  Vous pouvez attribuer une adresse IP publique (IPv4 uniquement)

  à n'importe quelle interface. Consultez Adresses IP publiques pour connaître les lignes directrices d'Azure concernant les adresses IP publiques, y compris comment créer, modifier ou supprimer une adresse IP publique.
- Un réseau virtuel avec quatre sous-réseaux (sauf si vous avez choisi un réseau existant)
- Un tableau de routage pour chaque sous-réseau (mis à jour s'il existe déjà)

  Les tableaux sont nommés nom du sous-réseau-ASAv-RouteTable.

  Chaque tableau de routage comprend les routes vers les trois autres sous-réseaux avec l'adresse IP ASA virtuel comme prochain saut. Vous pouvez choisir d'ajouter une route par défaut si le trafic doit atteindre d'autres sous-réseaux ou Internet.
- Un fichier de diagnostic de démarrage dans le compte de stockage sélectionné

  Le fichier de diagnostic de démarrage sera dans Blobs (objets binaires de grande taille).
- Deux fichiers dans le compte de stockage sélectionné sous Blobs et VHD (disques durs virtuels) de conteneur nommés *nom vm*-disk.vhd et *nom vm*-<uuid>.status
- Un compte de stockage (sauf si vous avez choisi un compte de stockage existant)

Remarque Lorsque vous supprimez une machine virtuelle, vous devez supprimer chacune de ces ressources individuellement, à l'exception de celles que vous souhaitez conserver.

Routage Azure

Le routage dans un réseau virtuel Azure est déterminé par la table de routage effective du réseau virtuel. La table de routage effective est une combinaison d'une table de routage système existante et de la table de routage définie par l'utilisateur.

Remarque 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 système.

Vous pouvez afficher et modifier la table de routage définie par l'utilisateur. Lorsque la table système et les tables définies par l'utilisateur sont combinées pour former la table de routage effective, la route la plus spécifique l'emporte et est liée à la table de routage définie par l'utilisateur. La table de routage système comprend une route par défaut (0.0.0.0/0) pointant vers la passerelle Internet de réseau virtuel d'Azure. La table de routage système comprend également des routes spécifiques vers les autres sous-réseaux définis avec le prochain saut pointant vers la passerelle d'infrastructure de réseau virtuel d'Azure.

Pour acheminer le trafic par le biais de l'ASA virtuel, le processus de déploiement d'ASA virtuel ajoute des routes sur chaque sous-réseau aux trois autres sous-réseaux en utilisant l'ASA virtuel comme saut suivant. Vous pouvez également ajouter une route par défaut (0.0.0.0/0) qui pointe vers l'interface ASA virtuel sur le sous-réseau. Cela enverra tout le trafic du sous-réseau par le biais d'ASA virtuel, ce qui peut exiger que des politiques ASA virtuel soient configurées à l'avance pour gérer ce trafic (éventuellement à l'aide de la NAT/PAT).

En raison des routes spécifiques existantes dans la table de routage système, vous devez ajouter des routes spécifiques à la table de routage définie par l'utilisateur pour pointer vers l'ASA virtuel comme prochain saut. Sinon, une route par défaut dans la table définie par l'utilisateur perdrait sa route plus précise dans la table de routage système et le trafic contournerait l'ASA virtuel.

Configuration du routeur pour les machines virtuelles dans le réseau virtuel

Le routage dans Azure Virtual Network dépend du tableau de routage en vigueur et non des paramètres de passerelle particuliers sur les clients. Les clients s'exécutant dans un réseau virtuel peuvent recevoir des routages par DHCP qui sont l'adresse .1 sur leurs sous-réseaux respectifs. Il s'agit d'un espace réservé qui sert uniquement à transmettre le paquet à la passerelle virtuelle de l'infrastructure du réseau virtuel. Une fois qu'un paquet quitte la machine virtuelle, il est acheminé selon la table de routage effective (telle que modifiée

par le tableau défini par l'utilisateur). La table de routage effective détermine le saut suivant, que le client virtuel ait ou non une passerelle configurée comme .1 ou comme adresse ASA virtuel

Les tableaux ARP de machine virtuelle Azure afficheront la même adresse MAC (1234.5678.9abc) pour tous les hôtes connus. Cela garantit que tous les paquets sortants d'une machine virtuelle Azure atteindront la passerelle Azure où la table de routage effective sera utilisée pour déterminer le chemin du paquet.

Remarque 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.

Adresses IP

Les informations suivantes s'appliquent aux adresses IP dans Azure :

- Vous devez utiliser DHCP pour définir les adresses IP des interfaces ASA virtuel.

  L'infrastructure Azure garantit que les interfaces de l'ASA virtuel reçoivent les adresses IP définies dans Azure.

- L'adresse IP privée de Management 0/0 se trouve dans le sous-réseau auquel il est associé.

  Une adresse IP publique peut être associée à cette adresse IP privée et la passerelle Internet Azure gérera les traductions NAT.

- Vous pouvez attribuer une adresse IP publique à n'importe quelle interface.

- Les adresses IP publiques qui sont dynamiques peuvent changer au cours d'un cycle d'arrêt/démarrage d'Azure. Cependant, elles sont persistantes pendant le redémarrage d'Azure et pendant le rechargement d'ASA virtuel.

- Les adresses IP publiques qui sont statiques ne changeront pas tant que vous ne les aurez pas modifiées dans Azure.

DNS

Tous les réseaux virtuels Azure ont accès à un serveur DNS intégré à l'adresse 168.63.129.16 que vous pouvez utiliser comme suit :

```
configure terminal
dns domain-lookup management
dns server-group DefaultDNS
 name-server 168.63.129.16
end
```

Vous pouvez utiliser cette configuration lorsque vous configurez les licences Smart et que vous n'avez pas configuré votre propre serveur DNS.

Mise en réseau accélérée (AN)

La fonctionnalité de mise en réseau accélérée (AN) d'Azure permet la virtualisation d'E/S à racine unique (SR-IOV) sur une VM, ce qui accélère la mise en réseau en permettant aux cartes réseau de la VM de contourner l'hyperviseur et d'accéder directement à la carte PCIe en dessous. L'AN améliore considérablement les performances de la VM en matière de débit et évolue également avec des cœurs supplémentaires (c.-à-d. des VM plus importantes).

L'AN est désactivée par défaut. Azure prend en charge l'activation de l'AN sur les machines virtuelles préprovisionnées. Vous devez simplement arrêter la VM dans Azure et mettre à jour la propriété de la carte réseau pour définir le paramètre *enableAcceleratedNetworking* sur « true » (vrai). Consultez la documentation de Microsoft Activer la mise en réseau accélérée sur les VM existantes. Redémarrez ensuite la VM.

Prise en charge du matériel Mellanox

Le nuage Microsoft Azure dispose de deux types de matériel qui prennent en charge la fonctionnalité AN : Mellanox 4 (MLX4) et Mellanox 5 (MLX5). L'ASA virtuel prend en charge AN pour le matériel Mellanox pour les instances suivantes de la version 9.15 :

- D3, D3_v2, DS3, DS3_v2
- D4, D4_v2, DS4, DS4_v2
- D5, D5_v2, DS5, DS5_v2
- D8_v3, D8s_v3
- D16_v3, D16s_v3
- F4, F4s
- F8, F8s, F8s_v2
- F16, F16s, F16s_v2

Remarque MLX4 (Mellanox 4) est également appelé connectx3 = cx3 et MLX5 (Mellanox 5) est également appelé connectx4 = cx4.

Vous ne pouvez pas spécifier quelle carte réseau Azure utilise MLX4 ou MLX5 pour votre déploiement de VM. Cisco vous recommande d'effectuer une mise à niveau vers la version 9.15 d'ASA virtuel ou une version ultérieure pour utiliser la fonctionnalité de mise en réseau accélérée.

Déployer l'ASA virtuel

Vous pouvez déployer l'ASA virtuel sur Microsoft Azure.

- Déployez l'ASA virtuel en tant que pare-feu autonome à l'aide d'Azure Resouce Manager sur le nuage public Azure standard et les environnements Azure pour le gouvernement. Consultez Déployer l'ASAv à partir d'Azure Resource Manager.

- Déployez l'ASA virtuel en tant que solution partenaire intégrée dans Azure à l'aide d'Azure Security Center. Les clients sensibles à la sécurité se voient proposer l'option ASA virtuel comme pare-feu pour protéger les charges de travail Azure. Les événements de sécurité et d'intégrité sont supervisés à partir d'un seul tableau de bord intégré. Consultez Déployer l'ASAv à partir d'Azure Security Center.
- Déployez une paire ASA virtuel à haute accessibilité à l'aide d'Azure Resource Manager. Pour assurer la redondance, vous pouvez déployer l'ASA virtuel 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. Consultez Déployer l'ASA virtuel pour la haute disponibilité à partir d'Azure Resource Manager, à la page 137.
- Déployez la paire ASA virtuel ou ASA virtuel à haute accessibilité avec un modèle personnalisé à l'aide d'une image gérée à partir d'un disque dur virtuel (disponible sur cisco.com). Cisco fournit un disque dur virtuel (VHD) compressé que vous pouvez charger vers Azure pour simplifier le processus de déploiement de l'ASA virtuel. À l'aide d'une image gérée et de deux fichiers JSON (un fichier de modèle et un fichier de paramètre), vous pouvez déployer et provisionner toutes les ressources pour l'ASA virtuel en une seule opération coordonnée. Pour utiliser le modèle personnalisé, consultez Déployer l'ASA virtuel à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 138.

Déployer l'ASA virtuel à partir d'Azure Resource Manager

La procédure suivante est une liste de haut niveau des étapes à suivre pour configurer Microsoft Azure sur l'ASA virtuel. Pour connaître les étapes détaillées de la configuration d'Azure, consultez Mise en route d'Azure.

Lorsque vous déployez l'ASA virtuel dans Azure, il génère automatiquement diverses configurations, telles que les ressources, les adresses IP publiques et les tables de routage. Vous pourrez gérer ces configurations après le déploiement. Par exemple, vous pouvez modifier la valeur du délai d'inactivité à partir de la valeur par défaut, qui est un délai d'expiration faible.

Procédure

Étape 1 Connectez-vous au portail Azure Resource Manager (ARM).

Le portail Azure affiche les éléments virtuels associés au compte et à l'abonnement actuels, quel que soit l'emplacement du centre de données.

Étape 2 Recherchez Cisco ASAv dans Marché, puis cliquez sur l'ASA virtuel que vous souhaitez déployer.

Étape 3 Configurez les paramètres de base.

a) Entrez un nom pour la machine virtuelle. Ce nom doit être unique dans votre abonnement Azure.

Important
Si votre nom n'est pas unique et que vous réutilisez un nom existant, le déploiement échouera.

b) Entrez votre nom d'utilisateur.

c) Choisissez un type d'authentification, **Password** (Mot de passe) ou **SSH public key** (Clé publique SSH).

Si vous choisissez **Password** (Mot de passe), saisissez un mot de passe et confirmez. Consultez la section Configuration du mot de passe pour connaître les consignes de complexité des mots de passe.

d) Choisissez votre type d'abonnement.

e) Choisissez un **Resource group** (Groupe de ressources).

Le groupe de ressources doit être le même que le groupe de ressources du réseau virtuel.

f) Choisissez votre emplacement.

L'emplacement doit être le même que pour votre réseau et votre groupe de ressources.

g) Cliquez sur **OK**.

Étape 4 Configurez les paramètres d'ASA virtuel.

a) Choisissez la taille de la machine virtuelle.

b) Choisissez un compte de stockage.

Vous pouvez utiliser un compte de stockage existant ou en créer un nouveau. L'emplacement du compte de stockage doit être le même que pour le réseau et la machine virtuelle.

c) Demandez une adresse IP publique en saisissant une étiquette pour l'adresse IP dans le champ Name (Nom), puis cliquez sur **OK**.

Azure crée une adresse IP publique dynamique par défaut, qui peut changer lorsque la machine virtuelle est arrêtée et redémarrée. Si vous préférez une adresse IP fixe, vous pouvez ouvrir l'adresse IP publique dans le portail et le faire passer d'une adresse dynamique à une adresse statique.

d) Ajoutez une étiquette DNS si vous le souhaitez.

Le nom de domaine complet sera votre étiquette DNS plus l'URL Azure : *<dnslabel>.<location>.cloupapp.azure.com*

e) Choisissez un réseau virtuel existant ou créez-en un nouveau.

f) Configurez les quatre sous-réseaux sur lesquels l'ASA virtuel sera déployé, puis cliquez sur **OK**.

Important
Chaque interface doit être associée à un sous-réseau unique.

g) Cliquez sur **OK**.

Étape 5 Affichez le résumé de la configuration, puis cliquez sur **OK**.

Étape 6 Affichez les conditions d'utilisation, puis cliquez sur **Create** (Créer).

Prochaine étape

- Poursuivez la configuration à l'aide des commandes de l'interface de ligne de commande disponibles pour une entrée par le biais du protocole SSH ou utilisez ASDM. Consultez la section Démarrer ASDM pour obtenir des instructions concernant l'accès à ASDM.

Déployer l'ASA virtuel à partir d'Azure Security Center

Microsoft Azure Security Center est une solution de sécurité pour Azure qui permet aux clients de protéger, de détecter et d'atténuer les risques de sécurité pour leurs déploiements dans le cloud. À partir du tableau de bord du centre de sécurité, les clients peuvent définir des politiques de sécurité, surveiller les configurations de sécurité et afficher les alertes de sécurité.

Le centre de sécurité analyse l'état de sécurité des ressources Azure pour identifier les failles de sécurité potentielles. Une liste de recommandations guide les clients dans le processus de configuration des contrôles

nécessaires, qui peut inclure le déploiement d'ASA virtuel en tant que solution de pare-feu pour les clients Azure.

En tant que solution intégrée dans le centre de sécurité, vous pouvez déployer rapidement l'ASA virtuel en quelques clics, puis surveiller les événements de sécurité et d'intégrité à partir d'un seul tableau de bord. La procédure suivante est une liste de niveaux supérieurs des étapes pour déployer l'ASA virtuel à partir du centre de sécurité. Pour des renseignements plus détaillés, consultez Azure Security Center.

Procédure

Étape 1 Connectez-vous au portail Azure.

Le portail Azure affiche les éléments virtuels associés au compte et à l'abonnement actuels, quel que soit l'emplacement du centre de données.

Étape 2 Dans le menu Microsoft Azure, choisissez **Security Center** (Centre de sécurité).

Si vous accédez au centre de sécurité pour la première fois, la lame **Welcome** (Bienvenue) s'ouvre. Choisissez **Yes! I want to Launch Azure Security Center** (Oui! Je souhaite lancer Azure Security Center) pour ouvrir la lame **Security Center** (Centre de sécurité) et activer la collecte de données.

Étape 3 Dans la lame **Security Center** (Centre de sécurité), choisissez la vignette **Policy** (Politique).

Étape 4 Dans la lame **Security policy** (Politique de sécurité), choisissez **Prevention policy** (Politique de prévention).

Étape 5 Dans la lame **Prevention policy** (Politique de prévention), activez les recommandations que vous souhaitez voir dans le cadre de votre politique de sécurité.

a) Définissez **Next generation firewall** (Pare-feu de nouvelle génération) sur **On** (Activé). Cela garantit que l'ASA virtuel est une solution recommandée dans le centre de sécurité.
b) Définissez d'autres recommandations selon vos besoins.

Étape 6 Revenez à la lame **Security Center** (Centre de sécurité) et à la vignette **Recommendations** (Recommandations).

Le centre de sécurité analyse périodiquement l'état de sécurité de vos ressources Azure. Lorsque le centre de sécurité identifie des failles de sécurité potentielles, il affiche les recommandations sur la lame **Recommendations** (Recommandations).

Étape 7 Sélectionnez la recommandation **Add a Next Generation Firewall** (Ajouter un pare-feu de nouvelle génération) dans la lame **Recommendations** (Recommandations) pour afficher plus de renseignements et/ou prendre des mesures pour résoudre le problème.

Étape 8 Choisissez **Create New** (Créer nouvelle) ou **Use existing solution** (Utiliser une solution existante), puis cliquez sur l'ASA virtuel que vous souhaitez déployer.

Étape 9 Configurez les paramètres de base.

a) Entrez un nom pour la machine virtuelle. Ce nom doit être unique dans votre abonnement Azure.

Important
Si votre nom n'est pas unique et que vous réutilisez un nom existant, le déploiement échouera.

b) Entrez votre nom d'utilisateur.
c) Choisissez un type d'autorisation, mot de passe ou clé SSH.

Si vous choisissez mot de passe, saisissez un mot de passe et confirmez. Consultez la section Configuration du mot de passe pour connaître les consignes de complexité des mots de passe.

d) Choisissez votre type d'abonnement.

e) Choisissez un groupe de ressources.

Le groupe de ressources doit être le même que le groupe de ressources du réseau virtuel.

f) Choisissez votre emplacement.

L'emplacement doit être le même que pour votre réseau et votre groupe de ressources.

g) Cliquez sur **OK**.

Étape 10 Configurez les paramètres d'ASA virtuel.

a) Choisissez la taille de la machine virtuelle.

L'ASA virtuel prend en charge Standard D3 et Standard D3_v2.

b) Choisissez un compte de stockage.

Vous pouvez utiliser un compte de stockage existant ou en créer un nouveau. L'emplacement du compte de stockage doit être le même que pour le réseau et la machine virtuelle.

c) Demandez une adresse IP publique en saisissant une étiquette pour l'adresse IP dans le champ Name (Nom), puis cliquez sur **OK**.

Azure crée une adresse IP publique dynamique par défaut, qui peut changer lorsque la machine virtuelle est arrêtée et redémarrée. Si vous préférez une adresse IP fixe, vous pouvez ouvrir l'adresse IP publique dans le portail et le faire passer d'une adresse dynamique à une adresse statique.

d) Ajoutez une étiquette DNS si vous le souhaitez.

Le nom de domaine complet sera votre étiquette DNS plus l'URL Azure : *<dnslabel>.<location>.cloupapp.azure.com*

e) Choisissez un réseau virtuel existant ou créez-en un nouveau.

f) Configurez les quatre sous-réseaux sur lesquels l'ASA virtuel sera déployé, puis cliquez sur **OK**.

Important
Chaque interface doit être associée à un sous-réseau unique.

g) Cliquez sur **OK**.

Étape 11 Affichez le résumé de la configuration, puis cliquez sur **OK**.

Étape 12 Affichez les conditions d'utilisation, puis cliquez sur **Create** (Créer).

Prochaine étape

- Poursuivez la configuration à l'aide des commandes de l'interface de ligne de commande disponibles pour une entrée par le biais du protocole SSH ou utilisez ASDM. Consultez la section Démarrer ASDM pour obtenir des instructions concernant l'accès à ASDM.
- Si vous avez besoin d'en savoir plus sur la façon dont les recommandations du centre de sécurité vous aident à protéger vos ressources Azure, consultez la documentation disponible dans le centre de sécurité.

Déployer l'ASA virtuel pour la haute disponibilité à partir d'Azure Resource Manager

La procédure suivante est une liste de niveaux supérieurs des étapes pour configurer une paire ASA virtuel à haute accessibilité sur Microsoft Azure. Pour connaître les étapes détaillées de la configuration d'Azure, consultez Mise en route d'Azure.

L'ASA virtuel à haute disponibilité dans Azure déploie deux ASA virtuel dans un ensemble de disponibilité et génère automatiquement diverses configurations, telles que les ressources, les adresses IP publiques et les tables de routage. Vous pourrez gérer ces configurations après le déploiement.

Procédure

Étape 1 Connectez-vous au portail Azure.

Le portail Azure affiche les éléments virtuels associés au compte et à l'abonnement actuels, quel que soit l'emplacement du centre de données.

Étape 2 Effectuez une recherche sur le Marché pour **Cisco ASAv**, puis cliquez sur **ASAv 4 NIC HA** (4 cartes réseau ASAv à haute disponibilité) pour déployer une configuration ASA virtuel de basculement.

Étape 3 Configurez les paramètres **Basics** (Base).

a) Saisissez un préfixe pour les noms de machine ASA virtuel. Les noms ASA virtuel auront le « préfixe »-A et le « préfixe »-B.

Important
Assurez-vous de ne pas utiliser un préfixe existant, sinon le déploiement échouera.

b) Saisissez un **nom d'utilisateur**.

Il s'agira du nom d'utilisateur administratif des deux machines virtuelles.

Important
L'**admin** du nom d'utilisateur n'est pas autorisé dans Azure.

c) Choisissez un type d'authentification pour les deux machines virtuelles, **Password** (Mot de passe) ou **SSH public key** (Clé publique SSH).

Si vous choisissez **Password** (Mot de passe), saisissez un mot de passe et confirmez. Consultez la section Configuration du mot de passe pour connaître les consignes de complexité des mots de passe.

d) Choisissez votre type d'abonnement.

e) Choisissez un **Resource group** (Groupe de ressources).

Choisissez **Create new (Créer nouveau)** pour créer un nouveau groupe de ressources, ou **Use exist** (Utiliser un groupe existant) pour sélectionner un groupe de ressources existant. Si vous utilisez un groupe de ressources existant, il doit être vide. Sinon, vous devez créer un nouveau groupe de ressources.

f) Choisissez votre **Location** (Emplacement).

L'emplacement doit être le même que pour votre réseau et votre groupe de ressources.

g) Cliquez sur **OK**.

Étape 4 Configurez les **Cisco ASAv settings** (Paramètres Cisco ASAv).

a) Choisissez la taille de la machine virtuelle.
b) Choisissez **Managed** (Géré) ou **Unmanaged OS disk** (Disque du système d'exploitation non géré) pour le stockage.

Important
Le mode haute disponibilité de l'ASA utilise toujours **Managed** (Géré).

Étape 5 Configurez les paramètres de l'**ASAv-A**.

a) (Facultatif) Choisissez **Create New** (Créer nouvelle) pour demander une adresse IP publique en saisissant une étiquette pour l'adresse IP dans le champ Name (Nom), puis cliquez sur **OK**. Choisissez **None** (Aucune) si vous ne souhaitez pas d'adresse IP publique.

Remarque
Azure crée une adresse IP publique dynamique par défaut, qui peut changer lorsque la machine virtuelle est arrêtée et redémarrée. Si vous préférez une adresse IP fixe, vous pouvez ouvrir l'adresse IP publique dans le portail et le faire passer d'une adresse dynamique à une adresse statique.

b) Ajoutez une étiquette DNS si vous le souhaitez.

Le nom de domaine complet sera votre étiquette DNS plus l'URL Azure : *<dnslabel>.<location>.cloupapp.azure.com*

c) Configurez les paramètres requis pour le compte de stockage pour les diagnostics de démarrage ASAv-A.

Étape 6 Répétez les étapes précédentes pour les paramètres **ASAv-B**.

Étape 7 Choisissez un réseau virtuel existant ou créez-en un nouveau.

a) Configurez les quatre sous-réseaux sur lesquels l'ASA virtuel sera déployé, puis cliquez sur **OK**.

Important
Chaque interface doit être associée à un sous-réseau unique.

b) Cliquez sur **OK**.

Étape 8 Affichez la configuration **Summary** (Résumé), puis cliquez sur **OK**.

Étape 9 Affichez les conditions d'utilisation, puis cliquez sur **Create** (Créer).

Prochaine étape

- Poursuivez la configuration à l'aide des commandes de l'interface de ligne de commande disponibles pour une entrée par le biais du protocole SSH ou utilisez ASDM. Consultez la section Démarrer ASDM pour obtenir des instructions concernant l'accès à ASDM.
- Consultez le chapitre « Basculement pour la haute disponibilité dans le nuage public » du Guide de configuration des opérations générales de la série ASA pour en savoir plus sur la configuration de l'ASA virtuel à haute disponibilité dans Azure.

Déployer l'ASA virtuel à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources

Vous pouvez créer vos propres images ASA virtuel personnalisées en utilisant une image de disque dur virtuel compressée disponible auprès de Cisco. Pour déployer à l'aide d'une image de disque dur virtuel, vous devez charger l'image de disque dur virtuel dans votre compte de stockage Azure. Ensuite, vous pouvez créer une

image gérée à l'aide de l'image disque chargée et d'un modèle d'Azure Resource Manager. Les modèles Azure sont des fichiers JSON qui contiennent des descriptions de ressources et des définitions de paramètres.

Avant de commencer

- Vous avez besoin du modèle JSON et du fichier de paramètres JSON correspondant pour votre déploiement de modèle ASA virtuel. Vous pouvez télécharger des fichiers de modèles à partir du référentiel GitHub à l'adresse :

  https://github.com/CiscoDevNet/cisco-asav/tree/master/deployment-templates/azure

- Pour des instructions sur la création d'un modèle et d'un fichier de paramètres, consultez Annexe : Exemple de modèle de ressource Azure, à la page 142.

- Cette procédure nécessite une machine virtuelle Linux existante dans Azure. Nous vous recommandons d'utiliser une machine virtuelle Linux temporaire (comme Ubuntu 16.04) pour charger l'image de disque dur virtuel compressée vers Azure. Cette image nécessite environ 50 Go de stockage lorsqu'elle est décompressée. De plus, vos délais de chargement vers le stockage Azure seront plus rapides à partir d'une machine virtuelle Linux dans Azure.

  Si vous devez créer une machine virtuelle, utilisez l'une des méthodes suivantes :

  - Créer une machine virtuelle Linux avec l'interface de ligne de commande Azure
  - Créer une machine virtuelle Linux dans le portail Azure

- Dans votre abonnement Azure, vous devez avoir un compte de stockage disponible à l'emplacement dans lequel vous souhaitez déployer l'ASA virtuel.

Procédure

Étape 1 Téléchargez l'image de disque dur virtuel compressée ASA virtuel à partir de la page https://software.cisco.com/download/home :

a) Accédez à **Products (produits)** > **Security (sécurité)** > **Firewalls (pare-feu)** > **Adaptive Security Appliances (ASA) (appareils de sécurité adaptables (ASA))** > **Adaptive Securtiy Appliance (ASA) Software (logiciel d'appareil de sécurité adaptable (ASA))**.

b) Cliquez sur **Adaptive Security Virtual Appliance (ASAv)** (appareil virtuel de sécurité adaptable (ASAv)).

Suivez les instructions pour télécharger l'image.

Par exemple, asav9-14-1.vhd.bz2

Étape 2 Copiez l'image de disque dur virtuel compressée sur votre machine virtuelle Linux dans Azure.

Il existe de nombreuses options que vous pouvez utiliser pour déplacer des fichiers vers Azure et à partir d'Azure. Cet exemple montre SCP ou copie sécurisée :

```
# scp /username@remotehost.com/dir/asav9-14-1.vhd.bz2 <linux-ip>
```

Étape 3 Connectez-vous à la machine virtuelle Linux dans Azure et accédez au répertoire où vous avez copié l'image de disque dur virtuel compressée.

Étape 4 Décompressez l'image de disque dur virtuel d'ASA virtuel.

Il existe de nombreuses options que vous pouvez utiliser pour décompresser des fichiers. Cet exemple montre l'utilitaire Bzip2, mais des utilitaires basés sur Windows fonctionneraient également.

```
# bunzip2 asav9-14-1.vhd.bz2
```

Étape 5 Chargez le disque dur virtuel dans un conteneur dans votre compte de stockage Azure. Vous pouvez utiliser un compte de stockage existant ou en créer un nouveau. Le nom du compte de stockage ne peut contenir que des lettres minuscules et des chiffres.

Il existe de nombreuses options que vous pouvez utiliser pour charger un disque virtuel sur votre compte de stockage, notamment AzCopy, l'API pour le stockage d'objets blob Azure, l'explorateur de stockage Azure, l'interface de ligne de commande Azure ou le portail Azure. Nous ne recommandons pas l'utilisation du portail Azure pour un fichier aussi volumineux que l'ASA virtuel.

L'exemple suivant montre la syntaxe en utilisant l'interface de ligne de commande Azure :

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

Étape 6 Créez une image gérée à partir du disque dur virtuel :

a) Dans le portail Azure, sélectionnez **Images**.
b) Cliquez sur **Add** (ajouter) pour créer une nouvelle image.
c) Fournir les renseignements suivants :

- **Subscription** (abonnement) : choisissez un abonnement dans la liste déroulante.
- **Resource group**(groupe de ressources) : choisissez un groupe de ressources existant ou créez-en.
- **Name** (nom) : saisissez un nom défini par l'utilisateur pour l'image gérée.
- **Region** (région) : choisissez la région dans laquelle la machine virtuelle est déployée.
- **OS type** (type de système d'exploitation) : choisissez **Linux** comme type de système d'exploitation.
- **VM genreation** (génération de la machine virtuelle) : choisissez **Gen 1**.

  Remarque
  Gen 2 n'est pas prise en charge.

- **Srorage blob** (objet biniare de stockage) : accédez au compte de stockage pour sélectionner le disque dur virtuel chargé.
- **Account type** (type de compte) : selon vos besoins, choisissez Standard HDD, Standard SSD ou Premium SSD dans la liste déroulante.

  Lorsque vous sélectionnez la taille de machine virtuelle planifiée pour le déploiement de cette image, assurez-vous que la taille de machine virtuelle prend en charge le type de compte sélectionné.
- **Host caching** (mise en mémoire cache de l'hôte) : choisissez Read/write (lecture/écriture) dans la liste déroulante.
- **Data disks**(disques de données) : laissez à la valeur par défaut; n'ajoutez pas de disque de données.

d) Cliquez sur **Create** (créer).

Attendez que le message **Successfully create image** (création d'image réussie) apparaisse sous l'onglet **Notifications**.

Remarque
Une fois que l'image gérée est créée, le disque dur virtuel chargé et le compte de stockage de charge peuvent être supprimés.

Étape 7 Obtenez l'ID de ressource de la nouvelle image gérée.

En interne, Azure associe chaque ressource à un ID de ressource. Vous aurez besoin de l'ID de ressource lorsque vous déployez de nouveaux pare-feu ASA virtuel à partir de cette image gérée.

a) Dans le portail Azure, sélectionnez **Images**.
b) Sélectionnez l'image gérée créée à l'étape précédente.
c) Cliquez sur **Overview** (aperçu) pour afficher les propriétés de l'image.
d) Copier l'**ID de ressource** dans le presse-papiers.

L'**ID de ressource** prend la forme de :

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>
/providers/Microsoft.Compute/<container>/ <vhdname>

Étape 8 Créez un pare-feu ASA virtuel en utilisant l'image gérée et un modèle de ressource :

a) Sélectionnez **New** (nouveau) et recherchez **Template Deployment** (déploiement de modèle) jusqu'à ce que vous puissiez le sélectionner dans les options.
b) Sélectionnez **Create** (créer).
c) Sélectionnez **Build your own template in the editor** (créer votre propre modèle dans l'éditeur).

Vous avez un modèle vide qui peut être personnalisé. Consultez Créer un modèle de ressources, à la page 143 pour un exemple de création d'un modèle

d) Collez votre code de modèle JSON personnalisé dans la fenêtre, puis cliquez sur **Save** (enregistrer).
e) Choisissez un **Subscription** (abonnement) dans la liste déroulante.
f) Choisissez un **Resource group** (groupe de ressources) existant ou créez-en un nouveau.
g) Choisissez un **Location** (emplacement) dans la liste déroulante.
h) Collez l'**ID de ressource** d'image gérée de l'étape précédente dans le champ **Vm Managed Image ID** (ID de l'image gérée de machine virtuelle).

Étape 9 Cliquez sur **Edit Parameters** (modifier les paramètres) en haut de la page **Custom Deployment** (déploiement personnalisé). Un modèle de paramètres est disponible pour la personnalisation.

a) Cliquez sur **Load file** (charger le fichier) et accédez au fichier de paramètres ASA virtuel personnalisé. Consultez Créer un fichier de paramètres, à la page 152 pour un exemple de création d'un modèle de paramètres.
b) Collez votre code de paramètres JSON personnalisé dans la fenêtre, puis cliquez sur **Save** (enregistrer).

Étape 10 Passer en revue les détails du déploiement personnalisé. Assurez-vous que les informations dans **Bases** (bases) et **Settings** (paramètres) correspondent à la configuration de déploiement attendue, y compris l'**ID de ressource**.

Étape 11 Passez en revue les conditions générales et cochez la case **I agree to the terms and conditions stated above** (j'accepte les conditions générales énoncées ci-dessus).

Étape 12 Cliquez sur **Purchase** (acheter) pour déployer un pare-feu ASA virtuel à l'aide de l'image gérée et d'un modèle personnalisé.

S'il n'y a aucun conflit dans vos fichiers de modèle et de paramètres, le déploiement devrait avoir réussi.

L'image gérée est disponible pour plusieurs déploiements dans le même abonnement et la même région.

Prochaine étape

- Poursuivez la configuration à l'aide des commandes CLI disponibles pour une entrée par le biais du protocole SSH ou utilisez ASDM. Consultez Démarrer ASDM, page 87 pour obtenir des instructions concernant l'accès à ASDM.

Annexe : Exemple de modèle de ressource Azure

Cette section décrit la structure d'un modèle Azure Resource Manager que vous pouvez utiliser pour déployer l'ASA virtuel. Un modèle de ressource Azure est un fichier JSON. Pour simplifier le déploiement de toutes les ressources requises, cet exemple comprend deux fichiers JSON :

- **Fichier de modèle** : il s'agit du principal fichier de ressources qui déploie tous les composants du groupe de ressources.
- **Fichier de paramètres** : ce fichier comprend les paramètres requis pour déployer avec succès l'ASA virtuel. Il comprend des détails tels que les informations sur le sous-réseau, le niveau et la taille de la machine virtuelle, le nom d'utilisateur et le mot de passe pour l'ASA virtuel, le nom du conteneur de stockage, etc. Vous pouvez personnaliser ce fichier pour votre environnement de déploiement Azure Stack Hub.

Format du fichier du modèle

Cette section décrit la structure d'un fichier de modèle Azure Resource Manager. L'exemple suivant montre une vue réduite d'un fichier de modèle et présente les différentes sections d'un modèle.

Fichier de modèle JSON d'Azure Resource Manager

```
{
    "$schema":
"http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "",
    "parameters": { },
    "variables": { },
    "resources": [ ],
    "outputs": { }
}
```

Le modèle est composé de JSON et d'expressions que vous pouvez utiliser pour construire des valeurs pour votre déploiement ASA virtuel. Dans sa structure la plus simple, un modèle contient les éléments suivants :

Tableau 19 : Éléments définis du fichier de modèle JSON d'Azure Resource Manager

Élément	Obligatoire	Description
$schema	Oui	Emplacement du fichier de schéma JSON qui décrit la version de la langue du modèle. Utilisez l'URL indiquée dans le schéma précédent.

Élément	Obligatoire	Description
contentVersion	Oui	Version du modèle (comme 1.0.0.0). Vous pouvez fournir n'importe quelle valeur pour cet élément. Lors du déploiement de ressources à l'aide du modèle, cette valeur peut être utilisée pour s'assurer que le bon modèle est utilisé.
paramètres	Non	Valeurs fournies lors du déploiement pour personnaliser le déploiement des ressources. Les paramètres permettent de saisir des valeurs au moment du déploiement. Ils ne sont pas obligatoires, mais sans eux, le modèle JSON déploiera les ressources avec les mêmes paramètres à chaque fois.
variables	Non	Valeurs utilisées comme fragments JSON dans le modèle pour simplifier les expressions linguistiques du modèle.
Ressources	Oui	Types de ressources déployées ou mises à jour dans un groupe de ressources.
sorties	Non	Valeurs retournées après le déploiement.

Vous pouvez utiliser les modèles JSON pour non seulement déclarer les types de ressources à déployer, mais également leurs paramètres de configuration associés. L'exemple suivant montre un modèle qui déploie un nouveau ASA virtuel.

Créer un modèle de ressources

Vous pouvez utiliser l'exemple ci-dessous pour créer votre propre modèle de déploiement à l'aide d'un éditeur de texte.

Procédure

Étape 1 Copiez le texte dans l'exemple suivant.

Exemple :

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string",
            "defaultValue": "ngfw",
            "metadata": {
                "description": "Name of the NGFW VM"
            }
        },
        "vmManagedImageId": {
            "type": "string",
            "defaultValue":
"/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage",

            "metadata": {
                "description": "The ID of the managed image used for deployment.
```

```
/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage"

            }
        },
        "adminUsername": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Username for the Virtual Machine. admin, Administrator among other
 values are disallowed - see Azure docs"
            }
        },
        "adminPassword": {
            "type": "securestring",
            "defaultValue" : "",
            "metadata": {
                "description": "Password for the Virtual Machine. Passwords must be 12 to 72 chars
 and have at least 3 of the following: Lowercase, uppercase, numbers, special chars"
            }
        },
        "vmStorageAccount": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "A storage account name (boot diags require a storage account).
Between 3 and 24 characters. Lowercase letters and numbers only"
            }
        },
        "virtualNetworkResourceGroup": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network's Resource Group"
            }
        },
        "virtualNetworkName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network"
            }
        },
        "mgmtSubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv management interface will attach to this subnet"
            }
        },
        "mgmtSubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "NGFW IP on the mgmt interface (example: 192.168.0.10)"
            }
        },
        "diagSubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv diagnostic0/0 interface will attach to this subnet"
            }
        },
        "diagSubnetIP": {
```

```
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "NGFW IP on the diag interface (example: 192.168.1.10)"
            }
        },
        "gig00SubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv Gigabit 0/0 interface will attach to this subnet"
            }
        },
        "gig00SubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The IP on the Gigabit 0/0 interface (example: 192.168.2.10)"
            }
        },
        "gig01SubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv Gigabit 0/1 interface will attach to this subnet"
            }
        },
        "gig01SubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The IP on the Gigabit 0/1 interface (example: 192.168.3.5)"
            }
        },
        "VmSize": {
            "type": "string",
            "defaultValue": "Standard_D3_v2",
            "allowedValues": [ "Standard_D3_v2" , "Standard_D3" ],
            "metadata": {
                "description": "NGFW VM Size (Standard_D3_v2 or Standard_D3)"
            }
        }
    },
    "variables": {

        "virtualNetworkID":
"[resourceId(parameters('virtualNetworkResourceGroup'),'Microsoft.Network/virtualNetworks',
parameters('virtualNetworkName'))]",

        "vmNic0Name":"[concat(parameters('vmName'),'-nic0')]",
        "vmNic1Name":"[concat(parameters('vmName'),'-nic1')]",
        "vmNic2Name":"[concat(parameters('vmName'),'-nic2')]",
        "vmNic3Name":"[concat(parameters('vmName'),'-nic3')]",

        "vmNic0NsgName":"[concat(variables('vmNic0Name'),'-NSG')]",

        "vmMgmtPublicIPAddressName": "[concat(parameters('vmName'),'nic0-ip')]",
        "vmMgmtPublicIPAddressType": "Static",
        "vmMgmtPublicIPAddressDnsName": "[variables('vmMgmtPublicIPAddressName')]"
    },
    "resources": [
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/publicIPAddresses",
```

```
            "name": "[variables('vmMgmtPublicIPAddressName')]",
            "location": "[resourceGroup().location]",
            "properties": {
              "publicIPAllocationMethod": "[variables('vmMgmtPublicIpAddressType')]",
              "dnsSettings": {
                "domainNameLabel": "[variables('vmMgmtPublicIPAddressDnsName')]"
              }
            }
        },
        {
            "apiVersion": "2015-06-15",
            "type": "Microsoft.Network/networkSecurityGroups",
            "name": "[variables('vmNic0NsgName')]",
            "location": "[resourceGroup().location]",
            "properties": {
                "securityRules": [
                    {
                        "name": "SSH-Rule",
                        "properties": {
                            "description": "Allow SSH",
                            "protocol": "Tcp",
                            "sourcePortRange": "*",
                            "destinationPortRange": "22",
                            "sourceAddressPrefix": "Internet",
                            "destinationAddressPrefix": "*",
                            "access": "Allow",
                            "priority": 100,
                            "direction": "Inbound"
                        }
                    },
                    {
                        "name": "SFtunnel-Rule",
                        "properties": {
                            "description": "Allow tcp 8305",
                            "protocol": "Tcp",
                            "sourcePortRange": "*",
                            "destinationPortRange": "8305",
                            "sourceAddressPrefix": "Internet",
                            "destinationAddressPrefix": "*",
                            "access": "Allow",
                            "priority": 101,
                            "direction": "Inbound"
                        }
                    }
                ]
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic0Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Network/networkSecurityGroups/',variables('vmNic0NsgName'))]",

                "[concat('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
```

```
                            "privateIPAddress" : "[parameters('mgmtSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('mgmtSubnetName'))]"
                            },
                            "publicIPAddress":{
                                "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
                            }
                        }
                    }
                ],
                "networkSecurityGroup": {
                    "id": "[resourceId('Microsoft.Network/networkSecurityGroups',
variables('vmNic0NsgName'))]"
                },
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic1Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('diagSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('diagSubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic2Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig00SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig00SubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
```

```
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic3Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig01SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig01SubnetName'))]"

                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[concat(parameters('vmStorageAccount'))]",
            "apiVersion": "2015-06-15",
            "location": "[resourceGroup().location]",
            "properties": {
              "accountType": "Standard_LRS"
            }
        },
        {
            "apiVersion": "2017-12-01",
            "type": "Microsoft.Compute/virtualMachines",
            "name": "[parameters('vmName')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Storage/storageAccounts/', parameters('vmStorageAccount'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic0Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic1Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic2Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic3Name'))]"
            ],
            "properties": {
                "hardwareProfile": {
                    "vmSize": "[parameters('vmSize')]"
                },
                "osProfile": {
                    "computername": "[parameters('vmName')]",
                    "adminUsername": "[parameters('AdminUsername')]",
                    "adminPassword": "[parameters('AdminPassword')]"
                },
                "storageProfile": {
                    "imageReference": {
                        "id": "[parameters('vmManagedImageId')]"
                    },
                    "osDisk": {
                        "osType": "Linux",
                        "caching": "ReadWrite",
                        "createOption": "FromImage"
                    }
```

```
                },
                "networkProfile": {
                    "networkInterfaces": [
                        {
                            "properties": {
                                "primary": true
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic0Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic1Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic2Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic3Name'))]"
                        }
                    ]
                },
                "diagnosticsProfile": {
                    "bootDiagnostics": {
                        "enabled": true,
                        "storageUri":
"[concat('http://',parameters('vmStorageAccount'),'.blob.core.windows.net')]"
                    }
                }
            }
        }
    ],
    "outputs": {  }
}
```

Étape 2 Enregistrez le fichier localement en tant que fichier JSON; par exemple, **azureDeploy.json**.

Étape 3 Modifiez le fichier pour créer un modèle correspondant à vos paramètres de déploiement.

Étape 4 Utilisez ce modèle pour déployer l'ASA virtuel comme décrit dans Déployer l'ASA virtuel à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 138.

Format du fichier des paramètres

Lorsque vous démarrez un nouveau déploiement, des paramètres sont définis dans votre modèle de ressources. Ces derniers doivent être saisis avant que le déploiement puisse commencer. Vous pouvez saisir manuellement les paramètres que vous avez définis dans votre modèle de ressources, ou vous pouvez placer les paramètres dans un fichier JSON de paramètres de modèle.

Le fichier de paramètres contient une valeur pour chaque paramètre affiché dans l'exemple des paramètres dans Créer un fichier de paramètres, à la page 152. Ces valeurs sont automatiquement transmises au modèle lors du déploiement. Vous pouvez créer plusieurs fichiers de paramètres pour différents scénarios de déploiement.

Pour le modèle ASA virtuel de cet exemple, le fichier de paramètres doit comporter les paramètres définis suivants :

Tableau 20 : Définitions des paramètresASA virtuel

Champ	Description	Exemple
vmName	Le nom que la machine ASA virtuel aura dans Azure.	cisco-asav
vmManagedImageId	ID de l'image gérée utilisée pour le déploiement. En interne, Azure associe chaque ressource à un ID de ressource.	/subscriptions/73d2537e-ca44-46aa-beb2-74ff1dd61b41/ resourceGroups/ew ManagedImages-rg/providers/Microsoft .Compute/ images/ASAv910-Managed-I mage
adminUsername	Le nom d'utilisateur pour la connexion à l'ASA virtuel. Il ne peut pas s'agir du nom réservé « admin ».	jdoe
adminPassword	Le mot de passe de l'administrateur. Il doit comporter de 12 à 72 caractères et inclure trois des éléments suivants : 1 minuscule, 1 majuscule, 1 chiffre, 1 caractère spécial.	Pw0987654321
vmStorageAccount	Votre compte de stockage Azure. Vous pouvez utiliser un compte de stockage existant ou en créer un nouveau. Le nom du compte de stockage doit comporter de 3 à 24 caractères et ne peut contenir que des lettres minuscules et des chiffres.	ciscoasavstorage
virtualNetworkResourceGroup	Le nom du groupe de ressources du réseau virtuel. L'ASA virtuel est toujours déployé dans un nouveau groupe de ressources.	ew-west8-rg
virtualNetworkName	Le nom du réseau virtuel.	ew-west8-vnet

Champ	Description	Exemple
mgmtSubnetName	L'interface de gestion sera associée à ce sous-réseau. Cela mappe à Nic0, le premier sous-réseau. Veuillez noter que cela doit correspondre à un nom de sous-réseau existant si vous rejoignez un réseau existant.	mgmt
mgmtSubnetIP	L'adresse IP de l'interface de gestion	10.8.0.55
gig00SubnetName	L'interface GigabitEthernet 0/0 se connectera à ce sous-réseau. Cela mappe à Nic1, le deuxième sous-réseau. Veuillez noter que cela doit correspondre à un nom de sous-réseau existant si vous rejoignez un réseau existant.	interne
gig00SubnetIP	L'adresse IP de l'interface GigabitEthernet 0/0. Il s'agit de la première interface de données de l'ASA virtuel.	10.8.2.55
gig01SubnetName	L'interface GigabitEthernet 0/1 s'associera à ce sous-réseau. Cela mappe à Nic2, le troisième sous-réseau. Veuillez noter que cela doit correspondre à un nom de sous-réseau existant si vous rejoignez un réseau existant.	externe
gig01SubnetIP	L'adresse IP de l'interface GigabitEthernet 0/1. Il s'agit de la deuxième interface de données d'ASA virtuel.	10.8.3.55
gig02SubnetName	L'interface GigabitEthernet 0/2 sera associée à ce sous-réseau. Cela mappe à Nic3, le quatrième sous-réseau. Veuillez noter que cela doit correspondre à un nom de sous-réseau existant si vous rejoignez un réseau existant.	dmz
gig02SubnetIP	L'adresse IP de l'interface GigabitEthernet 0/2. Il s'agit de la troisième interface de données d'ASA virtuel.	10.8.4.55

Champ	Description	Exemple
vmSize	La taille de machine virtuelle à utiliser pour la machine virtuelle ASA virtuel. Standard_D3_V2 et Standard_D3 sont prises en charge. Standard_D3_V2 est la valeur par défaut.	Standard_D3_V2 ou Standard_D3

Créer un fichier de paramètres

Vous pouvez utiliser l'exemple ci-dessous pour créer votre propre fichier de paramètres à l'aide d'un éditeur de texte.

Remarque L'exemple suivant concerne uniquement IPV4.

Procédure

Étape 1 Copiez le texte dans l'exemple suivant.

Exemple :

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "value": "cisco-asav1"
    },
    "vmManagedImageId": {
      "value":
"/subscriptions/33d2517e-ca88-46aa-beb2-74ffldb61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv-9.10.1-81-Managed-Image"

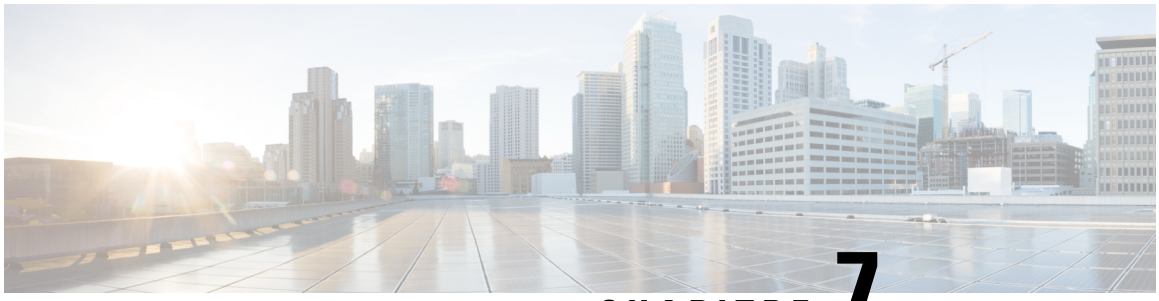
    },
    "adminUsername": {
      "value": "jdoe"
    },
    "adminPassword": {
      "value": "Pw0987654321"
    },
    "vmStorageAccount": {
      "value": "ciscoasavstorage"
    },
    "virtualNetworkResourceGroup": {
      "value": "ew-west8-rg"
    },
    "virtualNetworkName": {
      "value": "ew-west8-vn"
    },
    "mgmtSubnetName": {
      "value": "mgmt"
    },
```

```
    "mgmtSubnetIP": {
      "value": "10.8.3.77"
    },
    "gig00SubnetName": {
      "value": "inside"
    },
    "gig00SubnetIP": {
      "value": "10.8.2.77"
    },
    "gig01SubnetName": {
      "value": "outside"
    },
    "gig01SubnetIP": {
      "value": "10.8.1.77"
    },
    "gig02SubnetName": {
      "value": "dmz"
    },
    "gig02SubnetIP": {
      "value": "10.8.0.77"
    },
    "VmSize": {
      "value": "Standard_D3_v2"
    }
  }
}
```

Étape 2 Enregistrez le fichier localement en tant que fichier JSON; par exemple, **azureParameters.json**.

Étape 3 Modifiez le fichier pour créer un modèle correspondant à vos paramètres de déploiement.

Étape 4 Utilisez ce modèle de paramètre pour déployer l'ASA virtuel comme décrit dans Déployer l'ASA virtuel à partir d'Azure à l'aide d'un disque dur virtuel et d'un modèle de ressources, à la page 138.



CHAPITRE 7

Déployer la solution d'évolutivité automatique ASA virtuel sur Microsoft Azure

- Solution d'évolutivité automatique pour ASA virtuel sur Azure, à la page 155
- Télécharger le paquet de déploiement, à la page 157
- Composants de la solution d'évolutivité automatique, à la page 157
- Prérequis, à la page 159
- Déployer la solution d'évolutivité automatique, à la page 166
- Logique d'évolutivité automatique, à la page 182
- Journalisation et débogage de l'évolutivité automatique, à la page 182
- Lignes directrices et limites relatives à l'évolutivité automatique, à la page 184
- Dépannage, à la page 184
- Créer des fonctions Azure à partir du code source, à la page 185

Solution d'évolutivité automatique pour ASA virtuel sur Azure

Aperçu

L'évolutivité automatique d'ASA virtuel pour Azure est une implémentation complète sans serveur qui utilise l'infrastructure sans serveur fournie par Azure (application Logic, fonctions Azure, équilibreurs de charges, groupes de sécurité, ensemble d'évolutivité des machines virtuelles, etc.).

Certaines des fonctionnalités clés de l'évolutivité automatique d'ASA virtuel pour l'implémentation d'Azure comprennent :

- Le déploiement basé sur le modèle Azure Resource Manager (ARM).
- Prise en charge des mesures d'évolutivité en fonction du CPU.

Remarque Consultez Logique d'évolutivité automatique, à la page 182 pour de plus amples renseignements.

- Prise en charge du déploiement d'ASA virtuel et des zones de multi-disponibilité.

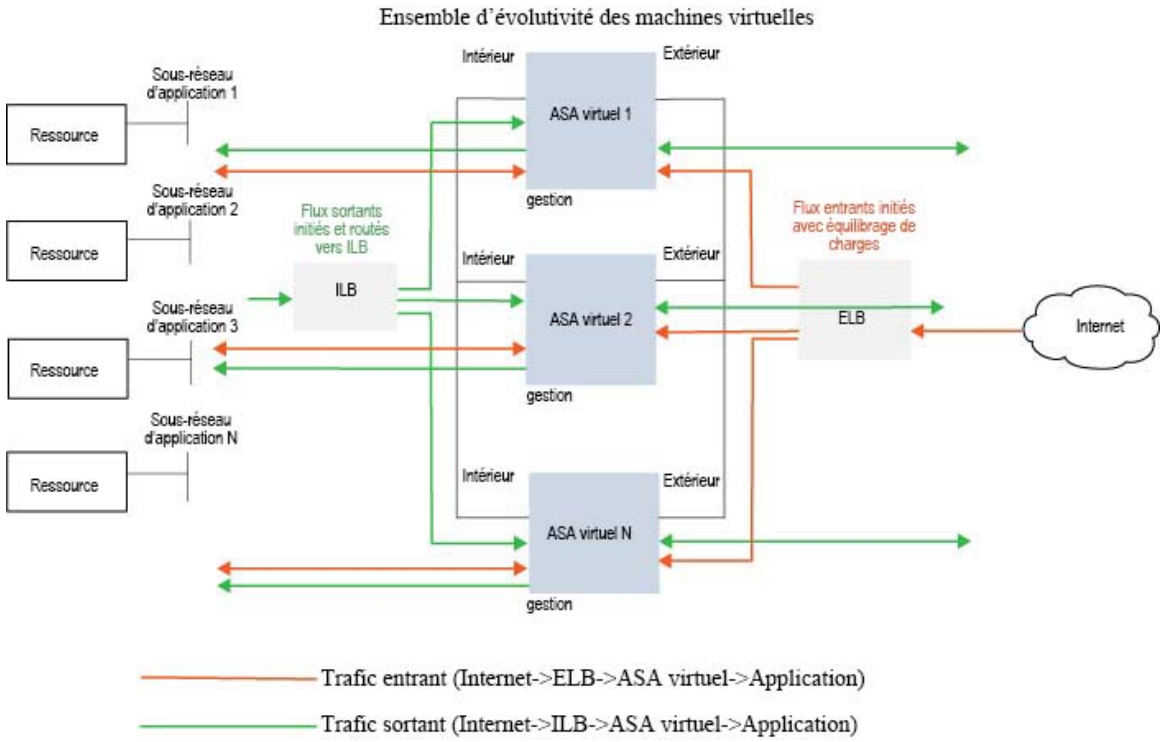
- La configuration entièrement automatisée s'applique automatiquement aux instances ASA virtuel soumise à l'évolutivité à la hausse.
- Prise en charge des équilibreurs de charges et des zones de multi-disponibilité.
- Prise en charge de l'activation et de la désactivation de la fonction d'évolutivité automatique.
- Cisco fournit un paquet de déploiement de l'évolutivité automatique pour Azure afin de faciliter le déploiement.

Scénario d'évolutivité automatique

L'évolutivité automatique d'ASA virtuel pour Azure est une solution d'évolutivité horizontale automatisée qui positionne un ensemble d'évolutivité ASA virtuel pris en sandwich entre un équilibreur de charges interne (ILB) Azure et un équilibreur de charges externe (ELB) Azure.

- L'ELB distribue le trafic d'Internet aux instances ASA virtuel dans l'ensemble d'évolutivité; le pare-feu transfère ensuite le trafic à l'application.
- L'ILB distribue le trafic Internet sortant d'une application aux instances ASA virtuel dans l'ensemble d'évolutivité; le pare-feu transfère ensuite le trafic à Internet.
- Un paquet réseau ne traversera jamais les deux équilibreurs de charges (interne et externe) en une seule connexion.
- Le nombre d'instances ASA virtuel dans l'ensemble d'évolutivité se verra évoluer et sera configuré automatiquement en fonction des conditions de charge.

Illustration 16 : Scénario d'évolutivité automatique ASA virtuel



Champ d'application

Ce document couvre les procédures détaillées pour déployer les composants sans serveur pour la solution d'évolutivité automatique d'ASA virtuel pour Azure.

Important

- Lisez le document entier avant de commencer le déploiement.
- Assurez-vous que les conditions préalables sont remplies avant de commencer le déploiement.
- Assurez-vous de suivre les étapes et l'ordre d'exécution décrits dans le présent document.

Télécharger le paquet de déploiement

La solution d'évolutivité automatique d'ASA virtuel pour Azure est un déploiement basé sur le modèle Azure Resource Manager (ARM) qui utilise l'infrastructure sans serveur fournie par Azure (application Logic, fonctions Azure, équilibreurs de charges, ensemble d'évolutivité des machines virtuelles, etc.)

Téléchargez les fichiers requis pour lancer la solution d'évolutivité automatique d'ASA virtuel pour Azure. Les scripts et les modèles de déploiement pour votre version sont disponibles dans le référentiel GitHub.

Attention Remarque : les scripts et les modèles de déploiement fournis par Cisco pour l'évolutivité automatique sont présentés à titre d'exemples de code source libre et ne font pas l'objet de l'assistance technique du TAC dans sa portée normale. Vérifiez régulièrement GitHub pour connaître les mises à jour et les instructions ReadMe.

Consultez Créer des fonctions Azure à partir du code source, à la page 185 pour obtenir des instructions sur la façon de créer le paquet *ASM_Function.zip*.

Composants de la solution d'évolutivité automatique

Les composants suivants constituent la solution d'évolutivité automatique d'ASA virtuel pour Azure.

Fonctions Azure (Function App)

Function App (Appli Fonction) est un ensemble de fonctions Azure. Voici les fonctionnalités de base :

- Sondez/communiquez régulièrement avec les mesures d'Azure.
- Surveillez la charge d'ASA virtuel et déclenchez les opérations d'évolutivité à la baisse/à la hausse.

Ces fonctions sont fournies sous forme de paquets zip compressé (voir Créer le paquet d'applications Azure Function, à la page 161). Les fonctions sont aussi distinctes que possible pour effectuer des tâches spécifiques et peuvent être mises à niveau au besoin pour améliorer et prendre en charge les nouvelles versions.

Orchestrateur (application Logic)

L'application Logic d'évolutivité automatique est un flux de travail, c'est-à-dire un ensemble d'étapes dans une séquence. Les fonctions Azure sont des entités indépendantes et ne peuvent pas communiquer entre elles. Cet orchestrateur séquence l'exécution de ces fonctions et échange des renseignements entre elles.

- L'application Logic est utilisée pour orchestrer et transmettre des renseignements entre les fonctions Azure d'évolutivité automatique.
- Chaque étape représente une fonction Azure d'évolutivité automatique ou une logique standard intégrée.
- L'application Logic est fournie sous forme de fichier JSON.
- L'application Logic peut être personnalisée au moyen du fichier d'interface graphique ou JSON.

Ensemble d'évolutivité des machines virtuelles (VMSS)

Le VMSS est un ensemble de machines virtuelles homologues, telles que les appareils ASA virtuel.

- Le VMSS est capable d'ajouter de nouvelles VM identiques à l'ensemble.
- Les nouvelles machines virtuelles (VM) ajoutées au VMSS sont automatiquement associées aux équilibreurs de charges, aux groupes de sécurité et aux interfaces réseau.
- Le VMSS a une fonctionnalité d'évolutivité automatique intégrée qui est désactivée pour ASA virtuel dans Azure.
- Vous ne devez pas ajouter ou supprimer des instances ASA virtuel dans le VMSS manuellement.

Modèle Azure Resource Manager (ARM)

Les modèles ARM sont utilisés pour déployer les ressources requises par l'évolutivité automatique d'ASA virtuel pour la solution Azure.

Évolutivité automatique d' pour Azure : le modèle ARM **azure_asav_autoscale.json** fournit des entrées pour les composants du gestionnaire d'évolutivité automatique, notamment :

- Function App (Appli Fonction) Azure
- Application Azure Logic
- L'ensemble d'évolutivité des machines virtuelles (VMSS)
- Équilibreurs de charges internes et externes.
- Goupes de sécurité et autres composants divers nécessaires au déploiement.

Important Le modèle ARM a des limites en ce qui concerne la validation des entrées des utilisateurs. Il est donc de votre responsabilité de valider les entrées pendant le déploiement.

Prérequis

Ressources Azure

Groupe de ressources

Un groupe de ressources existant ou nouvellement créé est requis pour déployer tous les composants de cette solution.

Remarque Enregistrez le nom du groupe de ressources, la région dans laquelle il est créé et l'ID d'abonnement Azure pour une utilisation ultérieure.

Mise en réseau

Assurez-vous qu'un réseau virtuel est disponible ou créé. Un déploiement de l'évolutivité automatique ne crée, ne modifie ni ne gère de ressources réseau.

L'ASA virtuel nécessite trois interfaces réseau. Par conséquent, votre réseau virtuel nécessite trois sous-réseaux pour :

1. Le trafic de gestion
2. Le trafic interne
3. Le trafic externe

Les ports suivants doivent être ouverts dans le groupe de sécurité réseau auquel les sous-réseaux sont connectés :

- SSH (TCP/22)

  Requis pour la sonde d'intégrité entre l'équilibreur de charges et ASA virtuel.

  Requis pour la communication entre les fonctions sans serveur et ASA virtuel.

- Protocole/ports spécifiques à l'application

  Requis pour toutes les applications des utilisateurs (par exemple, TCP/80, etc.).

Remarque Enregistrez le nom du réseau virtuel, le CIDR du réseau virtuel, les noms des 3 sous-réseaux et les adresses IP de passerelle des sous-réseaux externe et interne.

Préparer le fichier de configuration ASA

Préparez un fichier de configuration ASA virtuel et stockez-le dans un serveur http/https accessible par l'instance ASA virtuel. Il s'agit d'un format de fichier de configuration ASA standard. Un ASA virtuel qui évolue à la hausse téléchargera ce fichier et mettra à jour sa configuration.

Le fichier de configuration de l'ASA doit comporter les éléments suivants (au minimum) :

- Définissez l'attribution d'adresse IP DHCP pour toutes les interfaces.
- GigabitEthernet0/1 doit être l'interface « interne ».
- GigabitEthernet0/0 doit être l'interface « externe ».
- Définissez la passerelle vers l'interface interne et externe.
- Activez SSH sur les interfaces interne et externe à partir de l'adresse IP de l'utilitaire Azure (pour la sonde d'intégrité).
- Créez une configuration NAT pour transférer le trafic de l'interface externe vers l'interface interne.
- Créez une politique d'accès pour autoriser le trafic souhaité.
- Obtenez une licence la configuration. La facturation PAYG n'est pas prise en charge.

Remarque Il n'est pas nécessaire de configurer spécifiquement l'interface de gestion.

Voici un exemple de fichier de configuration ASA.

```
ASA Version 9.13(1)
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address dhcp setroute
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address dhcp setroute
!
route outside 0.0.0.0 0.0.0.0 10.12.3.1 2
!
route inside 0.0.0.0 0.0.0.0 10.12.2.1 3
!
ssh 168.63.129.0 255.255.255.0 outside
!
ssh 168.63.129.0 255.255.255.0 inside
!
object network webserver
host 10.12.2.5
object service myport
service tcp source range 1 65535 destination range 1 65535
access-list outowebaccess extended permit object myport any any log disable
access-group outowebaccess in interface outside
object service app
service tcp source eq www
nat (inside,outside) source static webserver interface destination static interface any
service app app
object network obj-any
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic obj-any interface destination static obj-any obj-any
configure terminal
dns domain-lookup management
```

```
policy-map global_policy
class inspection_default
inspect icmp
call-home
profile License
destination transport-method http
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
license smart
feature tier standard
throughput level 2G
license smart register idtoken <TOKEN>
: end
```

Créer le paquet d'applications Azure Function

La solution d'évolutivité automatique d'ASA virtuel nécessite que vous créiez un fichier d'archive : *ASM_Function.zip* qui fournit un ensemble de fonctions Azure distinctes sous la forme de paquet ZIP compressé.

Consultez Créer des fonctions Azure à partir du code source, à la page 185 pour obtenir des instructions sur la façon de créer le paquet *ASM_Function.zip*.

Ces fonctions sont aussi distinctes que possible pour effectuer des tâches spécifiques et peuvent être mises à niveau au besoin pour améliorer et prendre en charge les nouvelles versions.

Paramètres d'entrée

Le tableau suivant définit les paramètres du modèle et fournit un exemple. Une fois que vous avez choisi ces valeurs, vous pouvez utiliser ces paramètres pour créer l'appareil ASA virtuel lorsque vous déployez le modèle ARM dans votre abonnement Azure. Consultez Déployer le modèle ARM d'évolutivité automatique, à la page 166.

Tableau 21 : Paramètres du modèle

Nom du paramètre	Valeurs/Type autorisés	Description	Type de création de ressource
resourceNamePrefix	Chaîne* (3 à 10 caractères)	Toutes les ressources sont créées avec un nom contenant ce préfixe. Remarque : utilisez uniquement des lettres minuscules. Exemple : asav	New (Nouvelle)
virtualNetworkRg	Chaîne	Le nom du groupe de ressources du réseau virtuel. Exemple : cisco-virtualnet-rg	Existant
virtualNetworkName	Chaîne	Le nom du réseau virtuel (déjà créé). Exemple : cisco-virtualnet	Existant

Nom du paramètre	Valeurs/Type autorisés	Description	Type de création de ressource
mgmtSubnet	Chaîne	Le nom du sous-réseau de gestion (déjà créé). Exemple : cisco-mgmt-subnet	Existant
insideSubnet	Chaîne	Le nom du sous-réseau interne (déjà créé). Exemple : cisco-inside-subnet	Existant
internalLbIp	Chaîne	L'adresse IP de l'équilibreur de charges interne pour le sous-réseau interne (déjà créé). Exemple : 1.2.3.4	Existant
outsideSubnet	Chaîne	Le nom du sous-réseau externe (déjà créé). Exemple : cisco-outside-subnet	Existant
softwareVersion	Chaîne	La version ASA virtuel (sélectionné dans la liste déroulante pendant le déploiement). Par défaut : 914.1.0Autorisé : 914.1.0, 913.1.0	Existant
vmSize	Chaîne	Taille de l'instance ASA virtuel (sélectionné dans la liste déroulante pendant le déploiement).	S. O.
asaAdminUserName	Chaîne*	Nom d'utilisateur de l'utilisateur « admin » ASA virtuel. Les mots de passe doivent comporter de 12 à 72 caractères et doivent contenir : des minuscules, des majuscules, des chiffres et des caractères spéciaux; et ne doivent pas comporter plus de 2 caractères répétés. Cela **ne peut pas** être « admin ». Consultez Azure pour connaître les lignes directrices relatives au nom d'utilisateur de l'administrateur des VM. **Remarque** Il n'y a pas de vérification de conformité pour cela dans le modèle.	New (Nouvelle)

Nom du paramètre	Valeurs/Type autorisés	Description	Type de création de ressource
asaAdminUserPassword	Chaîne*	Mot de passe de l'utilisateur administrateur ASA virtuel. Les mots de passe doivent comporter de 12 à 72 caractères et doivent contenir : des minuscules, des majuscules, des chiffres et des caractères spéciaux; et ne doivent pas comporter plus de 2 caractères répétés. **Remarque** Il n'y a pas de vérification de conformité pour cela dans le modèle.	New (Nouvelle)
scalingPolicy	POLITIQUE-1 / POLITIQUE-2	**POLITIQUE-1** : l'évolutivité à la hausse sera déclenchée lorsque la charge moyenne de n'importe quel ASA virtuel dépassera le seuil d'évolutivité à la hausse pour la durée configurée. **POLITIQUE-2** : l'évolutivité à la hausse sera déclenchée lorsque la charge moyenne de tous les appareils ASA virtuel du groupe d'évolutivité automatique dépassera le seuil d'évolutivité à la hausse pour la durée configurée. Dans les deux cas, la logique d'évolutivité à la baisse reste la même : l'évolutivité à la baisse sera déclenchée lorsque la charge moyenne de tous les appareils ASA virtuel sera inférieure au seuil d'évolutivité à la baisse pour la durée configurée.	S. O.
scalingMetricsList	Chaîne	Mesures utilisées pour prendre la décision d'évolutivité. Autorisé : CPU Par défaut : CPU	S. O.

Nom du paramètre	Valeurs/Type autorisés	Description	Type de création de ressource
scaleInThreshold	Chaîne	Le seuil d'évolutivité à la baisse en pourcentage. Par défaut : 10 Lorsque la mesure ASA virtuel passe en dessous de cette valeur, l'évolutivité à la baisse est déclenchée. Consultez Logique d'évolutivité automatique, à la page 182.	S. O.
scaleOutThreshold	Chaîne	Le seuil d'évolutivité à la hausse en pourcentage. Par défaut : 80 Lorsque la mesure ASA virtuel dépasse cette valeur, l'évolutivité à la hausse est déclenchée. La valeur «scaleOutThreshold » doit toujours être **supérieure** à la valeur «scaleInThreshold ». Consultez Logique d'évolutivité automatique, à la page 182.	S. O.
minAsaCount	Nombre entier	Le nombre minimal d'instances ASA virtuel disponibles dans l'ensemble d'évolutivité à tout moment. Exemple : 2	S. O.
maxAsaCount	Nombre entier	Le nombre maximal d'instances ASA virtuel autorisées dans l'ensemble d'évolutivité. Exemple : 10 **Remarque** La logique d'évolutivité automatique ne vérifiera pas la plage de cette variable. Remplacez donc cette variable avec soin.	S. O.

Nom du paramètre	Valeurs/Type autorisés	Description	Type de création de ressource
metricsAverageDuration	Nombre entier	Sélectionnez une option dans la liste déroulante. Ce nombre représente la durée (en minutes) sur laquelle les mesures sont calculées en moyenne. Si la valeur de cette variable est 5 (c.-à-d. 5min), lorsque le gestionnaire d'évolutivité automatique est planifié, il vérifiera la moyenne des mesures des 5 dernières minutes et en fonction de cela, il prendra une décision en matière d'évolutivité. **Remarque** Seuls les chiffres 1, 5, 15 et 30 sont valides en raison des limites d'Azure.	S. O.
initDeploymentMode	LOT/ÉTAPE	Applicable principalement pour le premier déploiement ou lorsque l'ensemble d'évolutivité ne contient aucune instance ASA virtuel. BULK (LOT) : le gestionnaire d'évolutivité automatique tentera de déployer un nombre « minAsaCount » d'instances ASA virtuel en parallèle à la fois. STEP (ÉTAPE) : le gestionnaire d'évolutivité automatique déploiera le nombre «minAsaCount » d'appareils ASA virtuel un par un à chaque intervalle planifié.	
configurationFile	Chaîne	Le chemin d'accès au fichier de configuration ASA virtuel. Exemple : https://myserver/asavconfig/asaconfig.txt	S. O.
*Azure a des restrictions sur la convention de dénomination des nouvelles ressources. Vérifiez les limites ou utilisez simplement des minuscules. **N'utilisez pas d'espaces ni d'autres caractères spéciaux**.			

Déployer la solution d'évolutivité automatique

Déployer le modèle ARM d'évolutivité automatique

Évolutivité automatique de Utilisez le modèle ARM **azure_asav_autoscale.json** pour déployer les ressources requises par l'évolutivité automatique d'ASA virtuel pour Azure. Dans un groupe de ressources donné, le déploiement du modèle ARM crée les éléments suivants :

- Ensemble d'évolutivité des machines virtuelles (VMSS)
- Équilibreur de charges externe
- Équilibreur de charges interne
- Function App (Appli Fonction) Azure
- Application Logic
- Groupes de sécurité (pour les interfaces de données et de gestion)

Avant de commencer

- Téléchargez les modèles ARM à partir du référentiel GitHub (https://github.com/CiscoDevNet/cisco-asav/tree/master/autoscale/azure).

Procédure

Étape 1 Si vous devez déployer les instances ASA virtuel dans plusieurs zones Azure, modifiez le modèle ARM en fonction des zones disponibles dans la région de déploiement.

Exemple :

```
"zones": [
    "1",
    "2",
    "3"
],
```

Cet exemple montre la région « Centre des États-Unis » qui comporte 3 zones.

Étape 2 Modifiez les règles de trafic requises dans l'équilibreur de charges externe. Vous pouvez ajouter n'importe quel nombre de règles en étendant ce tableau « json ».

Exemple :

```
{
 "type": "Microsoft.Network/loadBalancers",
 "name": "[variables('elbName')]",
 "location": "[resourceGroup().location]",
 "apiVersion": "2018-06-01",
 "sku": {
```

```
          "name": "Standard"
        },
        "dependsOn": [
          "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"

        ],
        "properties": {
          "frontendIPConfigurations": [
            {
              "name": "LoadBalancerFrontEnd",
                "properties": {
                  "publicIPAddress": {
                    "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
                  }
                }
            }
          ],
          "backendAddressPools": [
            {
              "name": "backendPool"
            }
          ],
          "loadBalancingRules": [
            {
              "properties": {
                "frontendIPConfiguration": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/frontendIpConfigurations/LoadBalancerFrontend')]"
                },
                "backendAddressPool": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/backendAddressPools/BackendPool')]"
                },
                "probe": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/probes/lbprobe')]"
                },
                "protocol": "TCP",
                "frontendPort": "80",
                "backendPort": "80",
                "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
              },
              "Name": "lbrule"
            }
          ],
```

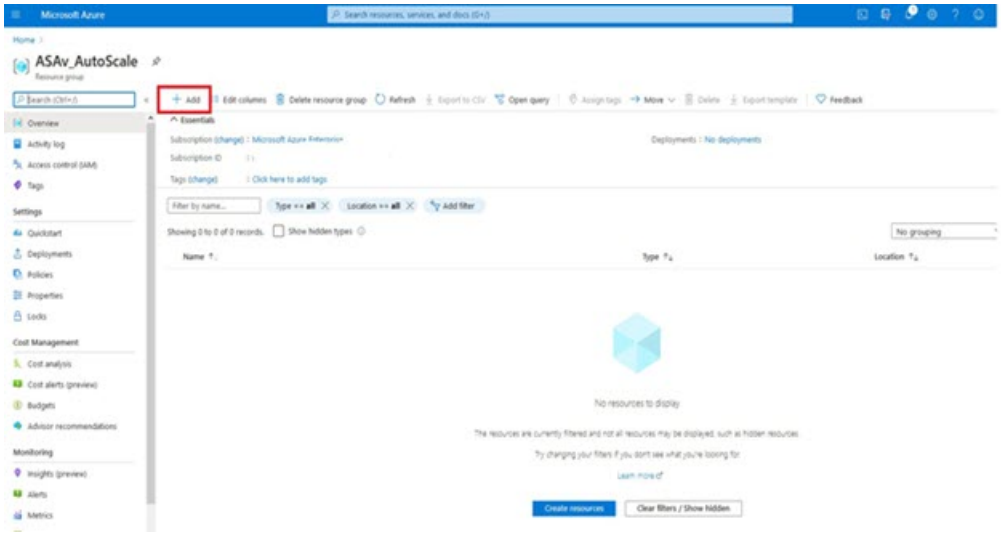
Remarque
Vous pouvez également le modifier à partir du portail Azure après le déploiement si vous préférez ne pas modifier ce fichier.

Étape 3 Connectez-vous au portail Microsoft Azure en utilisant le nom d'utilisateur et le mot de passe de votre compte Microsoft.

Étape 4 Cliquez sur **Resource groups** (Groupes de ressources) dans le menu des services pour accéder à la lame Resource Groups (Groupes de ressources). Vous verrez tous les groupes de ressources de votre abonnement répertoriés dans la lame.

Créez un nouveau groupe de ressources ou sélectionnez un groupe de ressources existant et vide; par exemple, *Évolutivité automatique_ASA virtuel*.

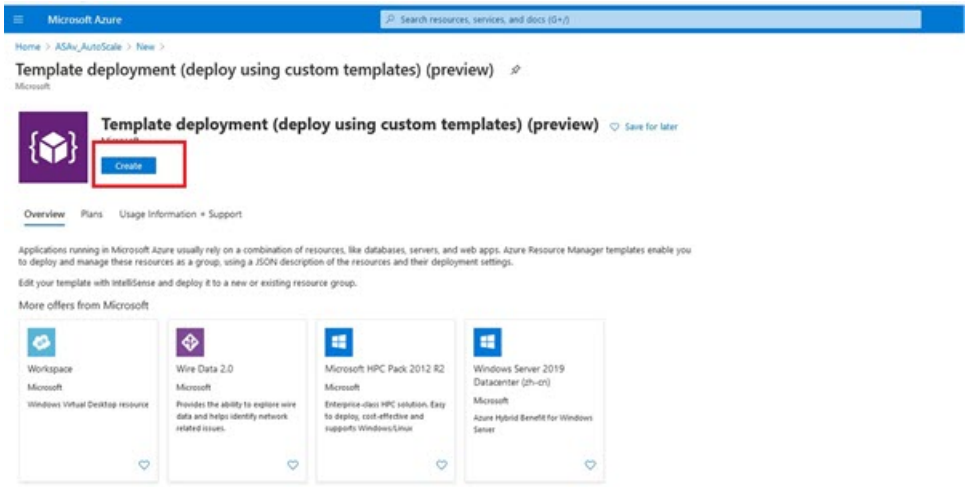
Illustration 17 : Portail Azure



Étape 5 Cliquez sur **Create a resource (+)** (Créer une ressource (+)) pour créer une nouvelle ressource pour le déploiement du modèle. La lame Create Resource Group (Créer un groupe de ressources) apparaît.

Étape 6 Dans **Search the Marketplace** (Rechercher sur le Marché), tapez **Template deployment (deploy using custom templates)** (Déploiement de modèles (déployez en utilisant des modèles personnalisés)), puis appuyez sur **Enter** (Entrée).

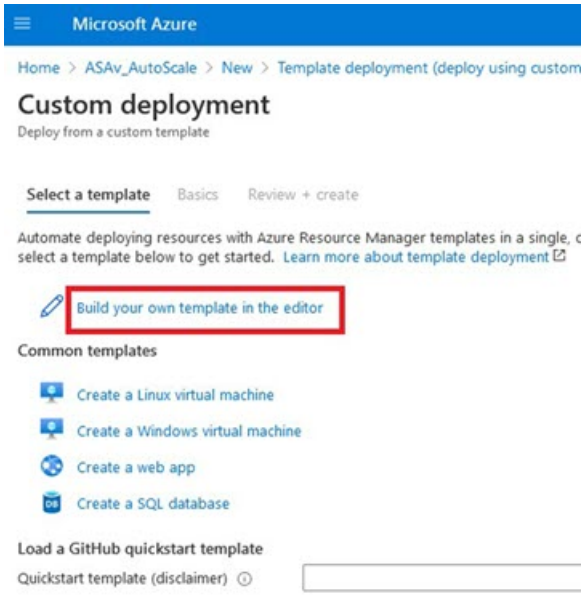
Illustration 18 : Déploiement du modèle personnalisé



Étape 7 Cliquez sur **Create** (créer).

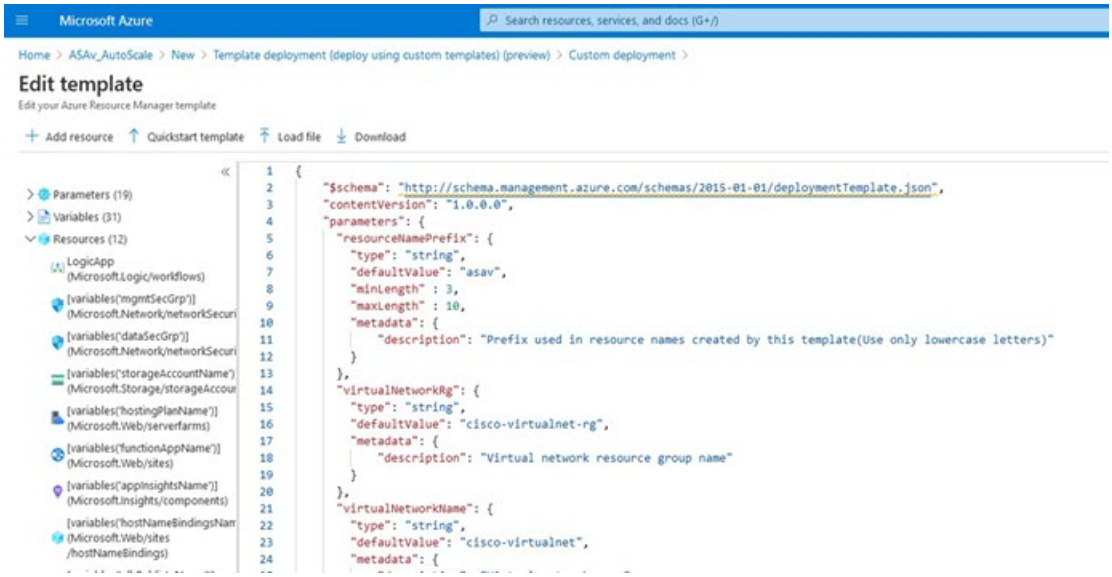
Étape 8 Il existe plusieurs options pour créer un modèle. Choisissez **Build your own template in editor** (Créer votre propre modèle dans l'éditeur).

Illustration 19 : Créer votre propre modèle



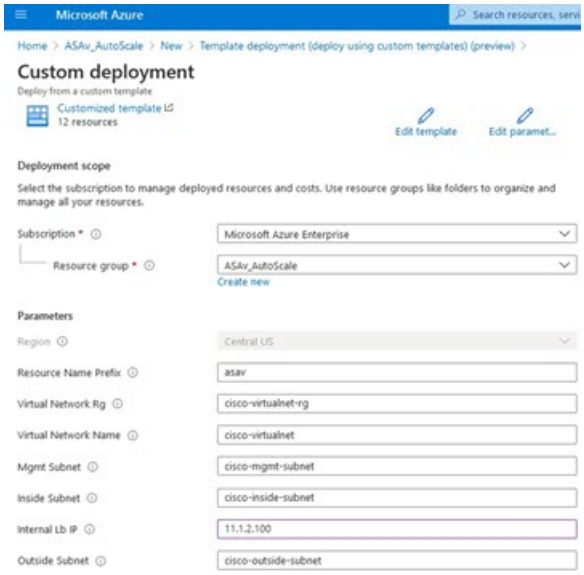
Étape 9 Dans la fenêtre **Edit template** (Modifier le modèle), supprimez tout le contenu par défaut et copiez le contenu à partir du fichier *azure_asav_autoscale.json* mis à jour et cliquez sur **Save** (Enregistrer).

Illustration 20 : Modifier le modèle



Étape 10 Dans la section suivante, renseignez tous les paramètres. Reportez-vous à Paramètres d'entrée, à la page 161 pour en savoir plus sur chaque paramètre, puis cliquez sur **Buy** (Acheter).

Illustration 21 : Paramètres du modèle ARM

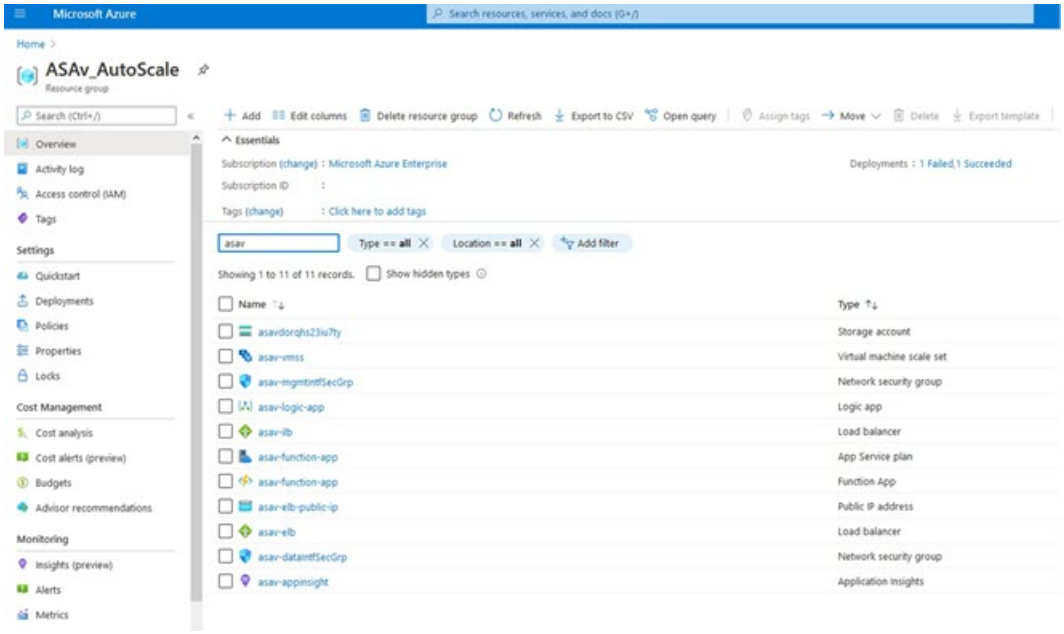


Remarque
Vous pouvez également cliquer sur **Edit Parameters** (Modifier les paramètres) et modifier le fichier JSON ou charger le contenu prérempli.

Le modèle ARM a des capacités de validation d'entrée limitées. Il est donc de votre responsabilité de valider l'entrée.

Étape 11 Lorsqu'un déploiement de modèle est réussi, il crée toutes les ressources requises pour l'évolutivité automatique d'ASA virtuel pour la solution Azure. Consultez les ressources dans la figure suivante. La colonne Type décrit chaque ressource, y compris l'application Logic, VMSS, les équilibreurs de charges, l'adresse IP publique, etc.

Illustration 22 : ASA Virtuel Déploiement du modèle d'évolutivité automatique



Déployer l'application Azure Function

Lorsque vous déployez le modèle ARM, Azure crée une application Function minimale, que vous devez ensuite mettre à jour et configurer manuellement avec les fonctions requises pour la logique Auto Scale Manager (gestionnaire d'évolutivité automatique).

Avant de commencer

- Créez le paquet *ASM_Function.zip*. Consultez Créer des fonctions Azure à partir du code source, à la page 185.

Procédure

Étape 1 Accédez à l'application Function que vous avez créée lors du déploiement du modèle ARM et vérifiez qu'aucune fonction n'est présente. Dans un navigateur, accédez à cette URL :

https://<Function App Name>.scm.azurewebsites.net/DebugConsole

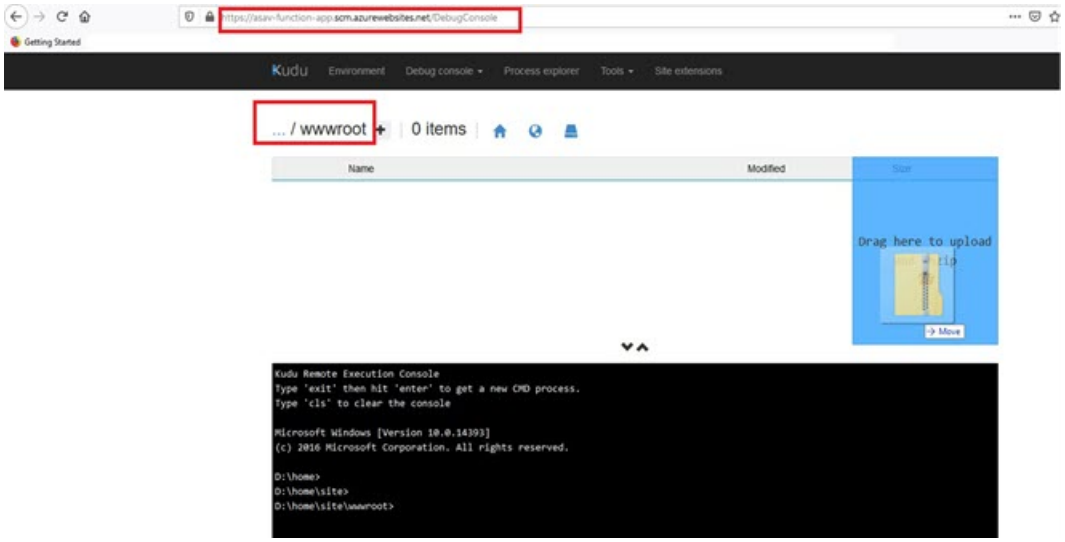
Par exemple dans Déployer le modèle ARM d'évolutivité automatique, à la page 166 :

https://asav-function-app.scm.azurewebsites.net/DebugConsole

Étape 2 Dans l'explorateur de fichiers, accédez à **site/wwwroot**.

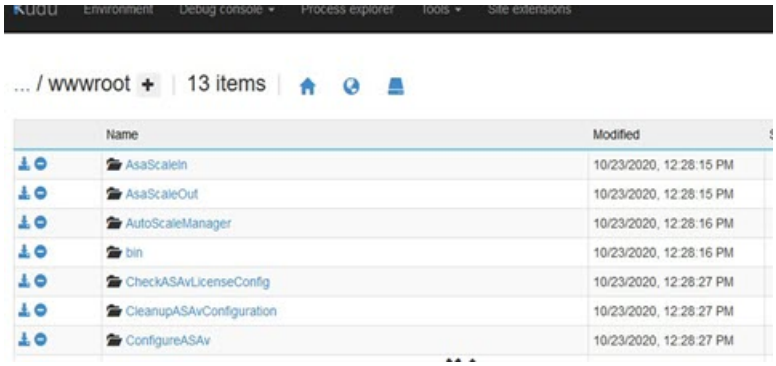
Étape 3 Glissez et déposez le fichier **ASM_Function.zip** dans le coin droit de l'explorateur de fichiers.

Illustration 23 : Charger les fonctions d'évolutivité automatique ASA Virtual



Étape 4 Une fois le chargement réussi, toutes les fonctions sans serveur devraient apparaître.

Illustration 24 : Fonctions sans serveur ASA Virtual

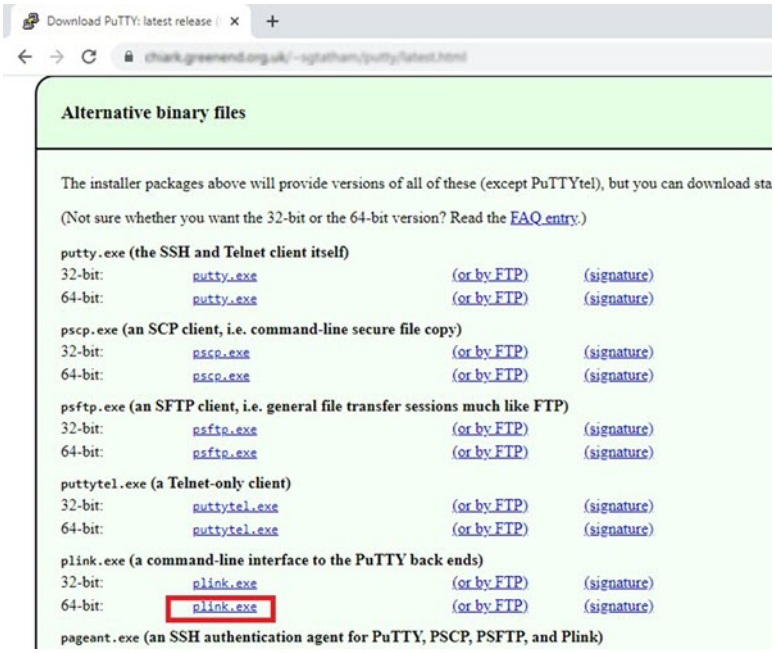


Étape 5 Téléchargez le client PuTTY SSH.

Les fonctions Azure doivent accéder à l'ASA virtuel par l'intermédiaire d'une connexion SSH. Cependant, les bibliothèques à code source libre utilisées dans le code sans serveur ne prennent pas en charge les algorithmes d'échange de clés SSH utilisés par l'ASA virtuel. Par conséquent, vous devez télécharger un client SSH préconçu.

Téléchargez l'interface CLI PuTTY sur le serveur principal PuTTY (*plink.exe*) à partir de www.putty.org.

Illustration 25 : Télécharger PuTTY



Étape 6 Renommez le fichier exécutable client SSH **plink.exe** en **asassh.exe**.

Étape 7 Glissez et déposez le fichier **asassh.exe** dans le coin droit de l'explorateur de fichiers, à l'emplacement où **ASM_Function.zip** a été chargé à l'étape précédente.

Étape 8 Vérifiez que le client SSH est présent avec l'application de fonction. Actualisez la page au besoin.

Ajustement de la configuration

Quelques configurations sont disponibles pour ajuster le gestionnaire d'évolutivité automatique ou à utiliser pour le débogage. Ces options ne sont pas exposées dans le modèle ARM, mais vous pouvez les modifier dans Function App (Appli Fonction).

Avant de commencer

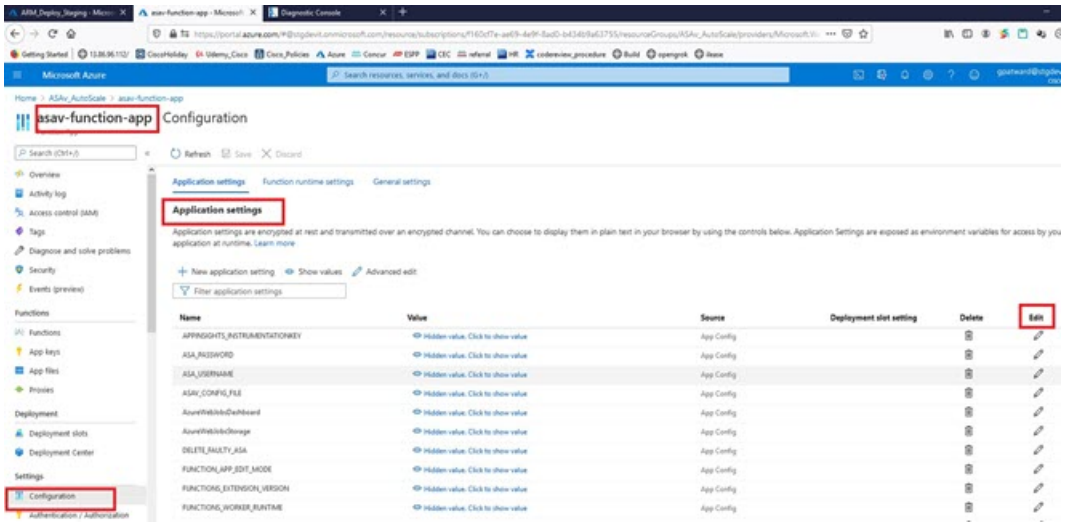
Remarque Cela peut être modifié à tout moment. Suivez cette séquence pour modifier les configurations.

- Désactiver Function App (Appli Fonction).
- Attendre la fin de la tâche planifiée existante.
- Modifier et enregistrer la configuration.
- Activer Function App (Appli Fonction).

Procédure

Étape 1 Dans le portail Azure, recherchez et sélectionnez l'application de fonction d'ASA virtuel.

Illustration 26 : ASA virtuelFunction App (Appli Fonction)



Étape 2 Les configurations transmises par le modèle ARM peuvent également être modifiées ici. Les noms des variables peuvent sembler différents de ceux du modèle ARM, mais vous pouvez facilement identifier le but de ces variables à partir de leur nom.

La plupart des options s'expliquent d'elles-mêmes à partir de leur nom. Par exemple :

- Nom de configuration : « DELETE_FAULTY_ASA » (Valeur par défaut : OUI)

  Pendant l'évolutivité à la hausse, une nouvelle instance ASA virtuel est lancée et configuré via le fichier de configuration. En cas d'échec de la de l'enregistrement, en fonction de cette option, le gestionnaire d'évolutivité automatique décidera de conserver cette instance ASA virtuel ou de la supprimer. (OUI : supprimer l'ASA virtuel défectueux/NON : conserver l'instance ASA virtuel même si la configuration échoue).

- Dans les paramètres de Function App (Appli Fonction), toutes les variables (y compris les variables contenant une chaîne sécurisée comme « password » (mot de passe)) peuvent être vues en texte clair par les utilisateurs qui ont accès à l'abonnement Azure.

  Si les utilisateurs rencontrent des problèmes de sécurité à ce sujet (par exemple, si un abonnement Azure est partagé entre des utilisateurs ayant des privilèges inférieurs au sein de l'organisation), un utilisateur peut utiliser le service *Key Vault* d'Azure pour protéger les mots de passe. Une fois cette configuration terminée, au lieu de fournir un « password » (mot de passe) en texte clair dans les paramètres de fonction, l'utilisateur doit fournir un identifiant sécurisé généré par le trousseau de clés où le mot de passe est stocké.

  Remarque
  Recherchez dans la documentation d'Azure pour trouver les bonnes pratiques pour sécuriser vos données d'application.

Configurer le rôle IAM dans l'ensemble d'évolutivité des machines virtuelles

Azure Identity and Access Management (IAM) est utilisé dans le cadre de la sécurité et du contrôle d'accès Azure pour gérer et contrôler l'identité d'un utilisateur. Les identités gérées pour les ressources d'Azure fournissent aux services Azure une identité gérée automatiquement dans Azure Active Directory.

Cela permet à Function App (Appli Fonction) de contrôler les ensembles d'évolutivité des machines virtuelles (VMSS) sans renseignements d'authentification explicites.

Procédure

Étape 1 Dans le portail Azure, accédez à VMSS.

Étape 2 Cliquez sur **Access control (IAM)** (Contrôle d'accès (IAM)).

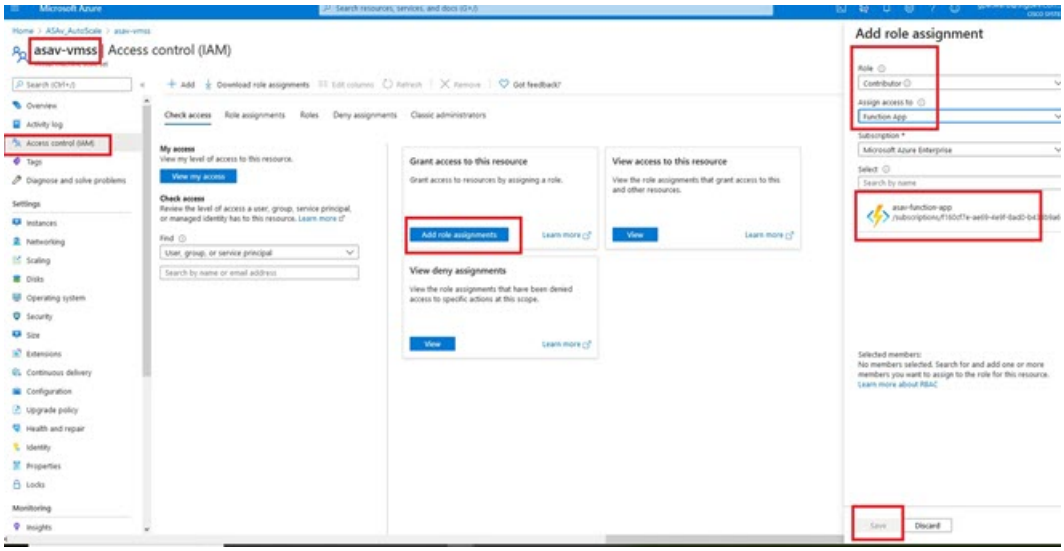
Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter une affectation de rôle

Étape 4 Dans la liste déroulante **Add Role Assignment** (Ajouter une affectation de rôle), choisissez **Contributor** (Contributeur).

Étape 5 Dans la liste déroulante **Assign access to** (Affecter l'accès à), sélectionnez **Function App** (Appli Fonction).

Étape 6 Sélectionnez l'application de fonction ASA virtuel.

Illustration 27 : Affectation du rôle AIM



Étape 7 Cliquez sur **Save** (enregistrer).

Remarque
Vous devez également vérifier qu'aucune instance ASA virtuel n'a encore été lancée.

Mettre à jour les groupes de sécurité

Le modèle ARM crée deux groupes de sécurité, un pour l'interface de gestion et un pour les interfaces de données. Le groupe de sécurité de gestion autorisera uniquement le trafic requis pour les activités de gestion d'ASA virtuel. Cependant, le groupe de sécurité de l'interface de données autorisera tout le trafic.

Procédure

Ajustez les règles des groupes de sécurité en fonction de la topologie et des besoins en application de vos déploiements.

Remarque
Le groupe de sécurité de l'interface de données doit autoriser au minimum le trafic SSH provenant des équilibreurs de charges.

Mettre à jour l'application Azure Logic

L'application Logic agit en tant qu'orchestrateur de la fonctionnalité d'évolutivité automatique. Le modèle ARM crée une application Logic minimale, que vous devez ensuite mettre à jour manuellement pour fournir les renseignements nécessaires à son fonctionnement en tant qu'orchestrateur de l'évolutivité automatique.

Procédure

Étape 1 À partir du référentiel, récupérez le fichier *LogicApp.txt* dans le système local et modifiez-le comme indiqué ci-dessous.

Important
Lisez et comprenez toutes ces étapes avant de continuer.

Ces étapes manuelles ne sont pas automatisées dans le modèle ARM afin que seule l'application Logic puisse être mise à niveau indépendamment plus tard.

a) Obligatoire : Recherchez et remplacez toutes les occurrences de « SUBSCRIPTION_ID » par les renseignements de votre ID d'abonnement.
b) Obligatoire : Recherchez et remplacez toutes les occurrences de « RG_NAME » par le nom de votre groupe de ressources.
c) Obligatoire : Recherchez et remplacez toutes les occurrences de « FUNCTIONAPPNAME » par le nom de votre application de fonction.

L'exemple suivant montre quelques-unes de ces lignes dans le fichier *LogicApp.txt* :

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
.
```

```
                        },
                        "Deploy_Changes_to_ASA": {
                            "inputs": {
                                "body": "@body('AutoScaleManager')",
                                "function": {
                                    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                                }
.
.
                        "DeviceDeRegister": {
                            "inputs": {
                                "body": "@body('AutoScaleManager')",
                                "function": {
                                    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                                }
                            },
                            "runAfter": {
                                "Delay_For_connection_Draining": [
```

d) (Facultatif) Modifiez l'intervalle de déclenchement ou conservez la valeur par défaut (5). Il s'agit de l'intervalle de temps auquel la fonctionnalité d'évolutivité automatique est déclenchée périodiquement. L'exemple suivant montre ces lignes dans le fichier *LogicApp.txt* :

```
"triggers": {
    "Recurrence": {
        "conditions": [],
        "inputs": {},
        "recurrence": {
            "frequency": "Minute",
            "interval": 5
        },
```

e) (Facultatif) Modifiez le temps de purge ou conservez la valeur par défaut (5). Il s'agit de l'intervalle de temps pour purger les connexions existantes de l'ASA virtuel avant de supprimer le périphérique pendant l'opération d'évolutivité à la baisse. L'exemple suivant montre ces lignes dans le fichier *LogicApp.txt* :

```
 "actions": {
      "Branch_based_on_Scale-In_or_Scale-Out_condition": {
          "actions": {
              "Delay_For_connection_Draining": {
                  "inputs": {
                      "interval": {
                          "count": 5,
                          "unit": "Minute"
                      }
```

f) (Facultatif) Modifiez le temps de refroidissement ou conservez la valeur par défaut (10). C'est le moment d'effectuer AUCUNE ACTION une fois le processus d'évolutivité à la hausse terminé. L'exemple suivant montre ces lignes dans le fichier *LogicApp.txt* :

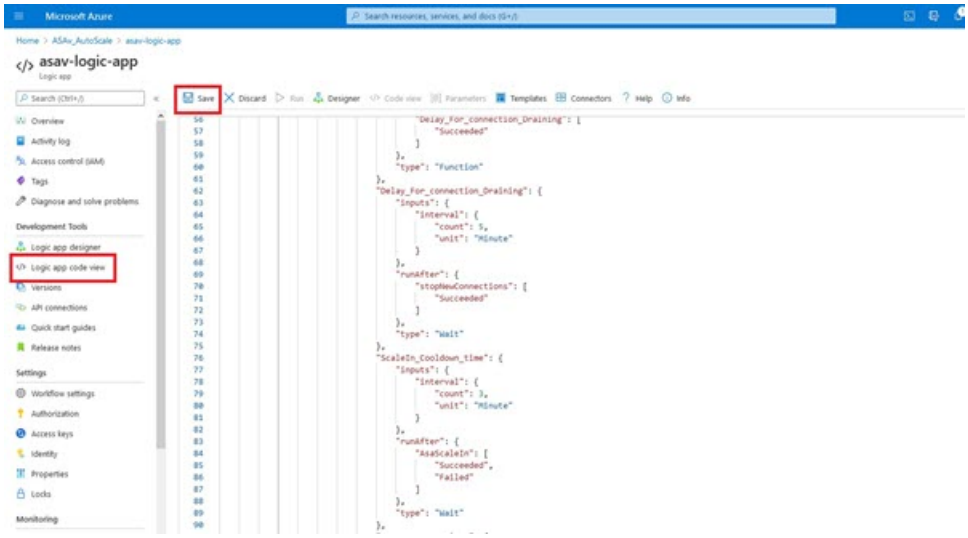
```
                "actions": {
                    "Branch_based_on_Scale-Out_or_Invalid_condition": {
                        "actions": {
                            "Cooldown_time": {
```

```
"inputs": {
    "interval": {
        "count": 10,
        "unit": "Second"
 }
```

Remarque
Ces étapes peuvent également être effectuées à partir du portail Azure. Pour en savoir plus, consultez la documentation Azure.

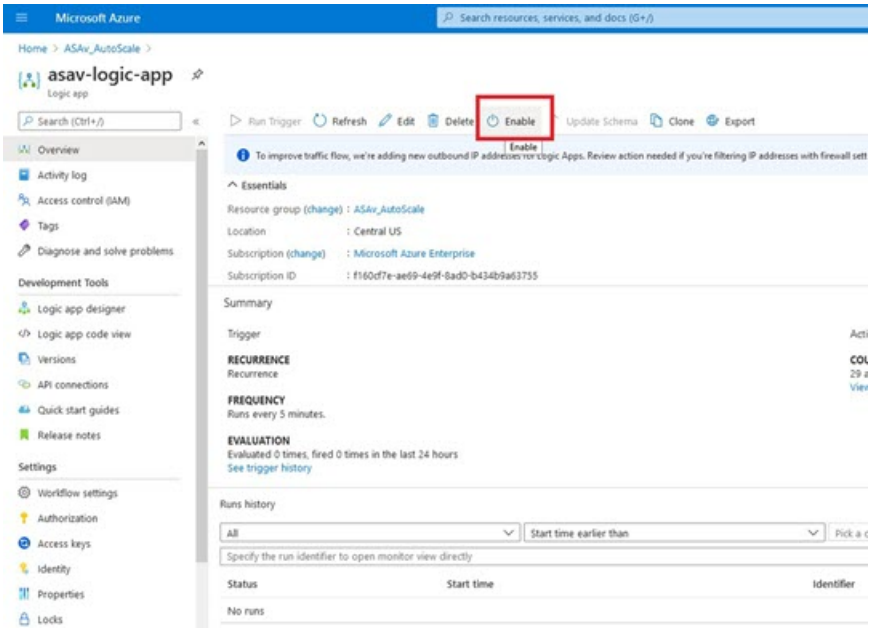
Étape 2 Accédez à **Logic App code view** (Vue du code d'application Logic), supprimez le contenu par défaut et collez le contenu du fichier modifié *LogicApp.txt*, puis cliquez sur **Save** (Enregistrer).

Illustration 28 : Vue du code d'application Logic



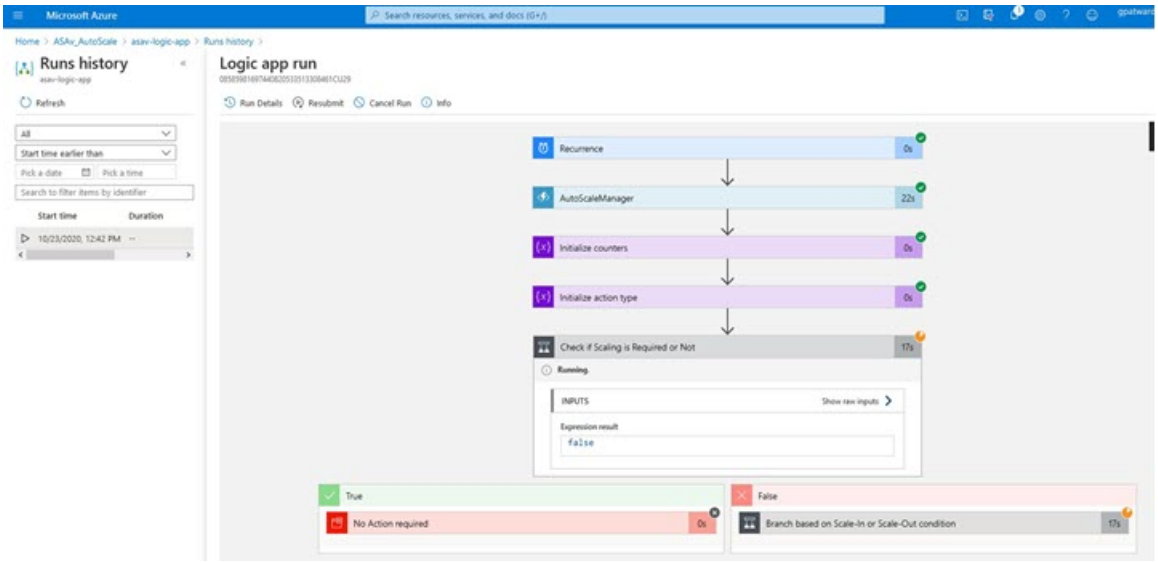
Étape 3 Lorsque vous enregistrez l'application Logic, elle est à l'état « Disabled » (Désactivé). Cliquez sur **Enable** (Activer) lorsque vous souhaitez démarrer le gestionnaire d'évolutivité automatique.

Illustration 29 : Activer l'application Logic



Étape 4 Une fois cette option activée, les tâches commencent à s'exécuter. Cliquez sur l'état « Running » (En cours d'exécution) pour voir l'activité.

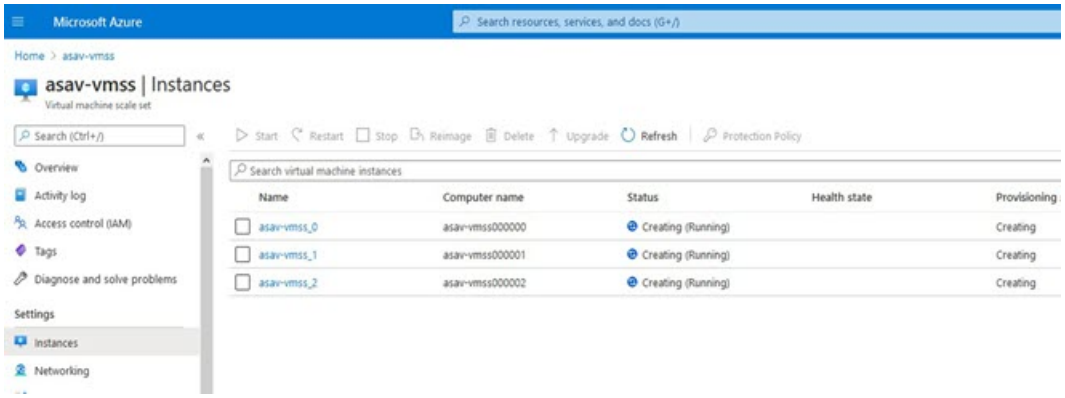
Illustration 30 : État en cours d'exécution de l'application Logic



Étape 5 Une fois que l'application Logic démarre, toutes les étapes liées au déploiement sont terminées.

Étape 6 Vérifiez dans le VMSS que des instances ASA virtuel sont créées.

Illustration 31 : Instances ASA virtuel en cours d'exécution



Dans cet exemple, trois instances ASA virtuel sont lancées parce que « minAsaCount » a été défini sur « 3 » et « initDeploymentMode » a été défini sur « BULK » dans le déploiement du modèle ARM.

Mettre à niveau l'ASA virtuel

La mise à niveau d'ASA virtuel est prise en charge uniquement sous la forme d'une mise à niveau d'image de l'ensemble d'évolutivité des machines virtuelles (VMSS). Par conséquent, vous mettez à niveau l'ASA virtuel par l'intermédiaire de l'interface API REST d'Azure.

Remarque Vous pouvez utiliser n'importe quel client REST pour mettre à niveau l'ASA virtuel.

Avant de commencer

- Obtenez la nouvelle version de l'image ASA virtuel disponible sur le marché (p. ex. : 914.001).
- Obtenez l'UGS utilisée pour déployer l'ensemble d'évolutivité d'origine (p. ex. : asav-azure-byol).
- Obtenez le nom défini pour le groupe de ressources et l'ensemble d'évolutivité des machines virtuelles.

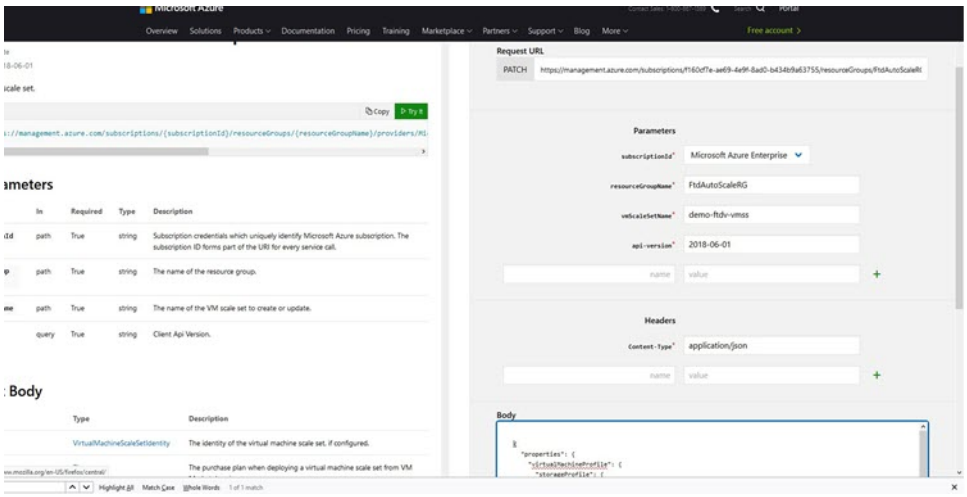
Procédure

Étape 1 Dans un navigateur, accédez à l'URL suivante :

https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0

Étape 2 Saisissez les détails dans la section Parameters (Paramètres).

Illustration 32 : Mettre à niveau l'ASA virtuel



Étape 3 Saisissez l'entrée JSON contenant la nouvelle version d'image d'ASA virtuel, l'UGS et le déclencheur d'exécution dans la section **Body** (Corps).

```
{
 "properties": {
        "virtualMachineProfile": {
              "storageProfile": {
                      "imageReference": {
                           "publisher": "cisco",
                           "offer": "cisco-asav",
                           "sku": "asav-azure-byol",
                            "version": "650.32.0"
                      }
                  },
            }
      }
}
```

Étape 4 Une réponse réussie d'Azure signifie que le VMSS a accepté la modification.

La nouvelle image sera utilisée dans les nouvelles instances d'ASA virtuel qui seront lancées dans le cadre de l'opération d'évolutivité à la hausse.

- Les instances d'ASA virtuel existantes continueront d'utiliser l'ancienne image logicielle tant qu'elles existent dans un ensemble d'évolutivité.
- Vous pouvez remplacer le comportement ci-dessus et mettre à niveau les instances d'ASA virtuel existantes manuellement. Pour ce faire, cliquez sur le bouton **Upgrade** (Mettre à niveau) dans VMSS. Il redémarrera et mettra à niveau les instances d'ASA virtuel sélectionnées. Vous devez réenregistrer et reconfigurer ces instances d'ASA virtuel mises à niveau manuellement. **Notez que cette méthode n'est PAS recommandée.**

Logique d'évolutivité automatique

Logique d'évolutivité à la hausse

- **POLITIQUE-1** : le protocole d'évolutivité à la hausse sera déclenché lorsque la charge moyenne de **n'importe quel** ASA virtuel dépasse le seuil d'évolutivité à la hausse pour la durée configurée.
- **POLITIQUE-2** : l'évolutivité à la hausse sera déclenchée lorsque la charge moyenne de **tous** les appareils ASA virtuel dépassera le seuil d'évolutivité à la hausse pour la durée configurée.

Logique d'évolutivité à la baisse

- Si l'utilisation du CPU de **tous** les appareils ASA virtuel passe en dessous du seuil d'évolutivité à la baisse configuré pour la durée configurée.

Notes

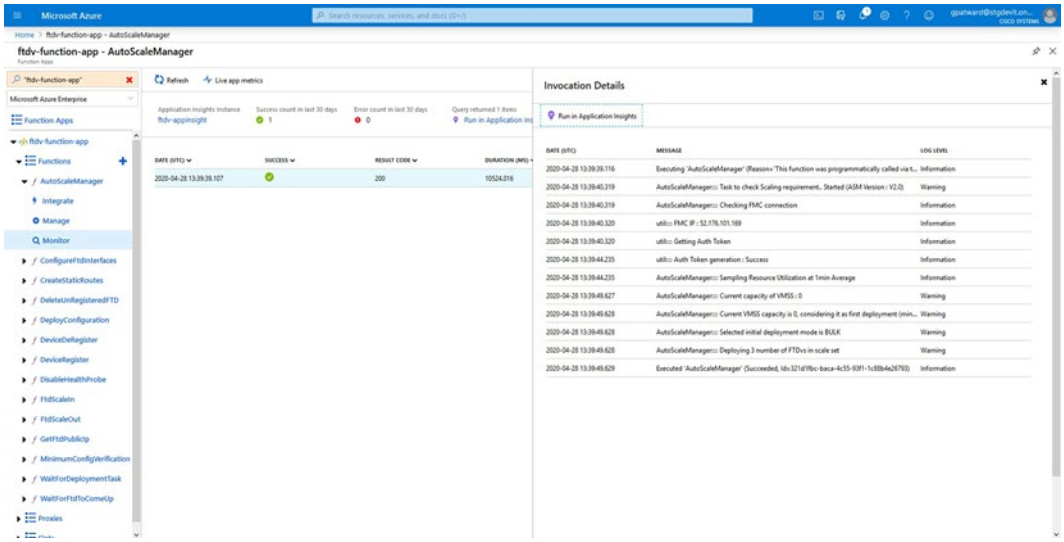
- L'évolutivité à la baisse/à la hausse se produit aux étapes de 1 (c.-à-d. que seul 1 ASA virtuel se verra évoluer à baisse/à la hausse à la fois).
- La logique ci-dessus est basée sur l'hypothèse que l'équilibreur de charges tentera de répartir également les connexions sur tous les appareils ASA virtuel et qu'en moyenne, tous les appareils ASA virtuel devraient être chargés de la même manière.

Journalisation et débogage de l'évolutivité automatique

Chaque composant du code sans serveur a son propre mécanisme de journalisation. En outre, des journaux sont publiés dans les données d'application.

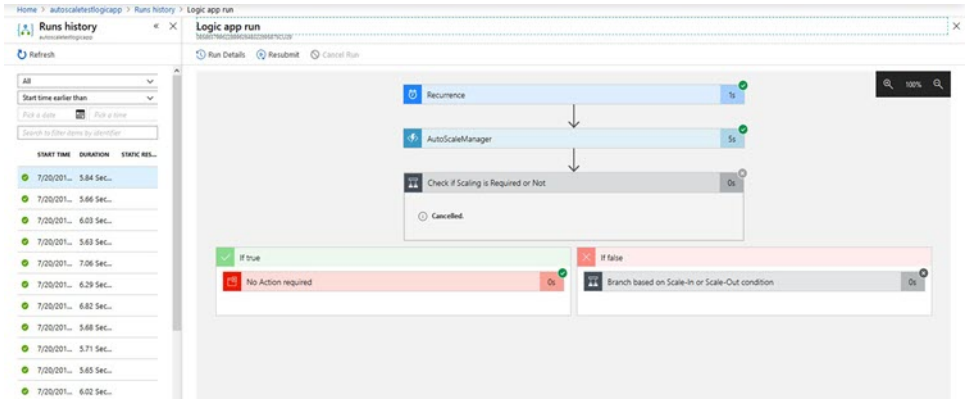
- Les journaux des fonctions Azure individuelles peuvent être consultés.

Illustration 33 : Journaux de fonction Azure



- Des journaux similaires pour chaque exécution de l'application Logic et de ses composants individuels peuvent être consultés.

Illustration 34 : Journaux d'exécution de l'application Logic



- Si nécessaire, toute tâche en cours dans l'application Logic peut être arrêtée/terminée à tout moment. Cependant, les appareils ASA virtuel en cours d'exécution sont lancés ou terminés et seront dans un état incohérent.
- Le temps nécessaire à chaque exécution ou tâche individuelle peut être vu dans l'application Logic.
- Function App (Appli Fonction) peut être mise à niveau à tout moment en chargeant un nouveau fichier zip. Arrêtez l'application Logic et attendez que toutes les tâches soient terminées avant de mettre à niveau Function App (Appli Fonction).

Lignes directrices et limites relatives à l'évolutivité automatique

Prenez connaissance des lignes directrices et des limites suivantes lors du déploiement de l'évolutivité automatique d'ASA virtuel pour Azure :

- Les décisions d'évolutivité sont basées sur l'utilisation du processeur.
- L'interface de gestion de l'ASA virtuel est configurée pour avoir une adresse IP publique.
- Seul IPv4 est pris en charge.
- Le modèle ARM a des capacités de validation d'entrée limitées. Il est donc de votre responsabilité de prévoir une validation d'entrée appropriée.
- L'administrateur Azure peut voir des données sensibles (comme les informations d'authentification et les mots de passe de l'administrateur) en texte brut dans l'environnement d'application de fonction. Vous pouvez utiliser le service *Azure Key Vault* pour sécuriser des données sensibles.
- Toute modification de la configuration ne sera pas automatiquement reflétée sur les instances déjà en cours d'exécution. Ces modifications ne seront reflétées que sur les prochains périphériques intégrés. Toutes les modifications de ce type doivent être transférées manuellement vers les périphériques existants.
- Si vous rencontrez des problèmes lors de la mise à jour manuelle de la configuration sur les instances existantes, nous vous recommandons de supprimer ces instances du groupe d'évolutivité et de les remplacer par de nouvelles.

Dépannage

Voici des scénarios d'erreurs courants et des conseils de débogage pour l'évolutivité automatique de l'ASA virtuel pour Azure :

- Impossible de connecter avec le protocole SSH à l'ASA virtuel : vérifiez si un mot de passe complexe est transmis à l'ASA virtuel au moyen du modèle; vérifiez si les groupes de sécurité autorisent les connexions SSH.
- Échec du contrôle de l'intégrité de l'équilibreur de charges : vérifiez si l'ASA virtuel répond à SSH sur les interfaces de données; vérifiez les paramètres du groupe de sécurité.
- Problèmes de trafic : vérifiez les règles de l'équilibreur de charges, les règles NAT/les routes statiques configurées dans ASA virtuel; vérifiez les détails d'Azure Virtual Network, des sous-réseaux et de la passerelle fournis dans le modèle et les règles du groupe de sécurité.
- L'application Logic n'a pas pu accéder à VMSS : vérifiez si la configuration du rôle IAM dans VMSS est correcte.
- L'application Logic fonctionne très longtemps : vérifiez l'accès SSH sur les appareils ASA virtuel qui évoluent à la hausse; vérifiez l'état des appareils ASA virtuel dans Azure VMSS.
- La fonction Azure lance une erreur liée à l'ID d'abonnement : vérifiez que vous avez un abonnement par défaut sélectionné dans votre compte.

- Échec de l'opération d'évolutivité à la baisse : parfois, Azure prend considérablement de temps pour supprimer une instance dans de telles situations. L'opération d'évolutivité à la baisse peut expirer et signaler une erreur; mais l'instance sera peut-être supprimée.
- Avant de modifier la configuration, assurez-vous de désactiver l'application Logic et d'attendre la fin de toutes les tâches en cours.

Créer des fonctions Azure à partir du code source

Configuration système requise

- Ordinateur de bureau/portable Microsoft Windows.
- Visual Studio (testé avec Visual Studio 2019 version 16.1.3)

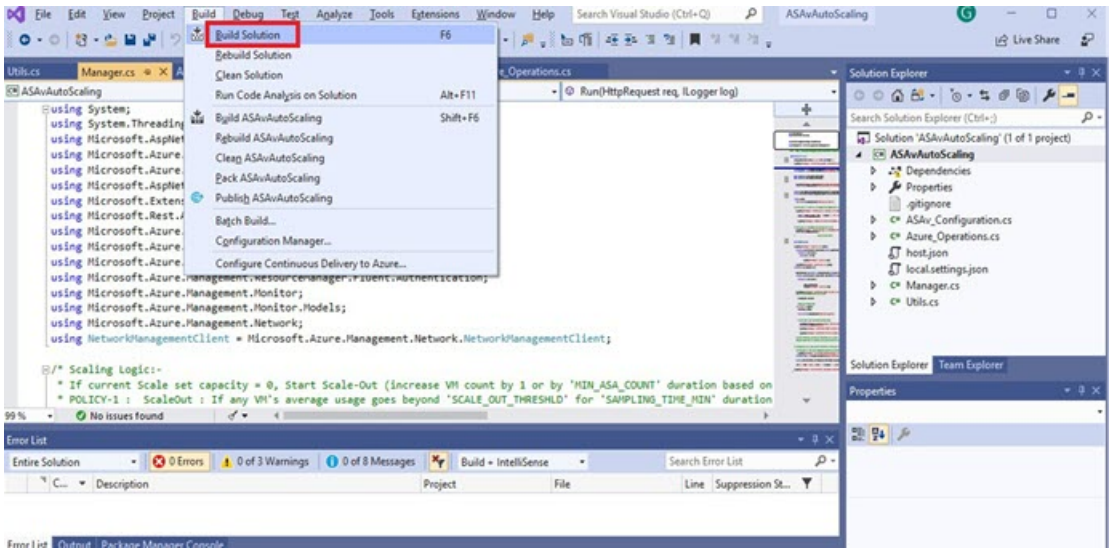
Remarque Les fonctions Azure sont écrites à l'aide de C#.

- La charge de travail « Azure Development » (développement Azure) doit être installée dans Visual Studio.

Créer avec Visual Studio

1. Téléchargez le dossier « code » sur la machine locale.
2. Accédez au dossier «ASA AutoScaling ».
3. Ouvrez le fichier de projet «ASAAutoScaling.csproj » dans Visual Studio.
4. Utilisez la procédure standard de Visual Studio pour nettoyer et créer.

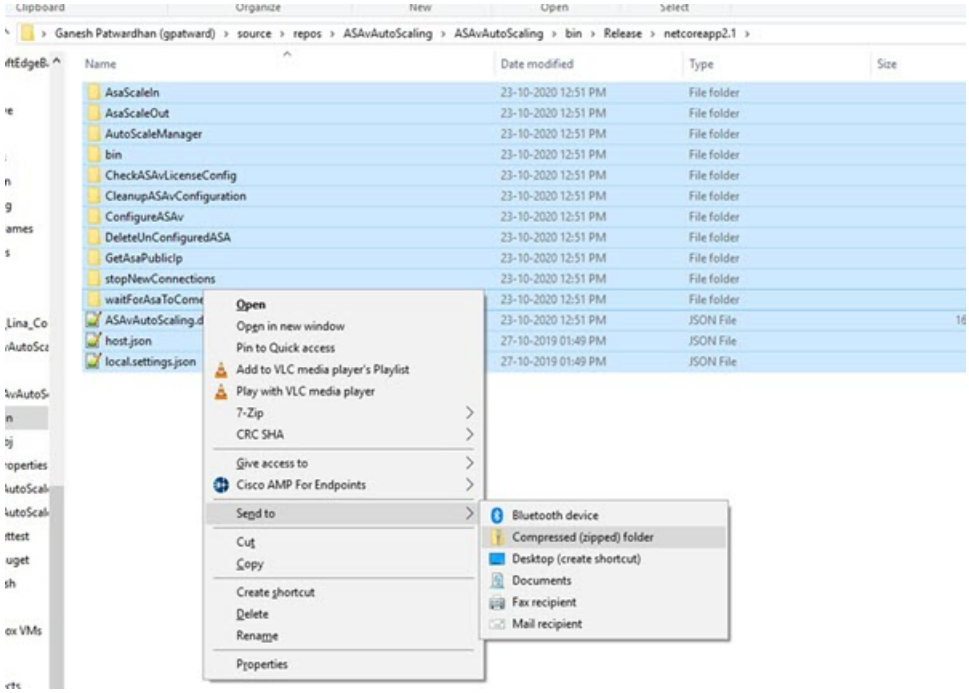
Illustration 35 : Création dans Visual Studio

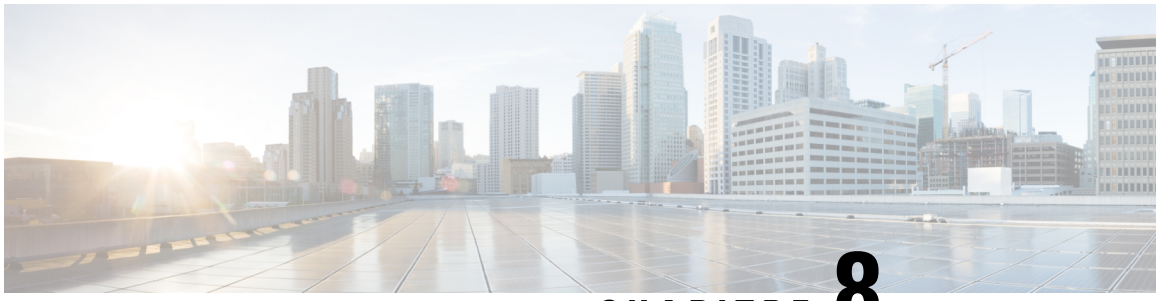


5. Une fois que la version est compilée avec succès, accédez au dossier **\bin\Release\netcoreapp2.1**.

6. Sélectionnez tout le contenu, cliquez sur **Send to (envoyer à)** > **Compressed (zipped) folder (dossier compressé (zip))**, et enregistrez le fichier ZIP sous le nom *ASM_Function.zip*.

Illustration 36 : Créer ASM_Function.zip





CHAPITRE 8

Déployer l'ASA virtuel sur Rackspace Cloud

Vous pouvez déployer l'ASA virtuel sur Rackspace Cloud

Important À partir de la version 9.13(1), toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge. Cela permet aux clients ASA virtuel d'exécuter une grande variété d'empreintes de ressources de VM.

- Aperçu, à la page 187
- Prérequis, à la page 188
- Réseau Rackspace Cloud, à la page 189
- Configuration Rackspace Day 0 (jour 0), à la page 190
- Déployer l'ASA virtuel , à la page 192
- Utilisation et rapport d'utilisation du processeur (CPU), à la page 194

Aperçu

Rackspace est un chef de file d'expertise et de services gérés pour toutes les principales technologies de cloud public et privé. Rackspace Cloud est un ensemble de produits et de services informatiques en nuage facturés sur une base d'informatique utilitaire.

Vous pouvez déployer l'ASA virtuel pour Rackspace en tant qu'appliance virtuelle dans Rackspace Cloud. Ce chapitre explique comment installer et configurer un appareil ASA virtuel à instance unique.

Les types d'instances dans Rackspace Cloud sont appelés *flavors* (enveloppes). Le terme « enveloppe » fait référence à la combinaison de la taille de la RAM, des vCPU, du débit réseau (facteur RXTX) et de l'espace disque d'un serveur. Le tableau suivant répertorie les enveloppes Rackspace adaptées au déploiement d'ASA virtuel.

Tableau 22 : Enveloppes prises en charge par Rackspace

Saveur	Attributs		Bande passante agrégée
	vCPU	Mémoire (Go)	
général 1-2	2	2	400 Mbit/sec
général 1-4	4	4	800 Mbit/s

Saveur	Attributs		Bande passante agrégée
	vCPU	Mémoire (Go)	
général 1-8	8	8	1,6 Gbit/s
calcul 1-4	2	3,75	312,5 Mbit/s
calcul 1-8	4	7,5	625 Mbit/s
calcul 1-15	8	15	1,3 Gb/s
mémoire 1-15	2	15	625 Mbit/s
mémoire 1-15	4	30	1,3 Gb/s
mémoire 1-15	8	60	2,5 Gbit/sec

À propos des enveloppes Rackspace

Les enveloppes des serveurs en nuage virtuels Rackspace se répartissent dans les classes suivantes :

- **Objectif général v1**
  - Utile pour une gamme de scénarios, des charges de travail à usage général aux sites Web hautes performances.
  - Les vCPU sont surexploités et peuvent être en « rafales »; en d'autres termes, il y a plus de vCPU alloués aux serveurs en nuage sur un hôte physique qu'il y a de fils CPU physiques.
- **Calcul v1**
  - Optimisé pour les serveurs Web, les serveurs d'applications et d'autres charges de travail exigeantes en CPU.
  - Les vCPU sont « réservés »; en d'autres termes, il n'y a jamais plus de vCPU alloués aux serveurs en nuage sur un hôte physique qu'il y a de fils CPU physiques sur cet hôte.
- **Mémoire v1**
  - Recommandé pour les charges de travail exigeantes en mémoire.
- **E/S v1**
  - Idéal pour les applications et les bases de données hautes performances qui bénéficient d'E/S de disque rapide.

Prérequis

- Créez un compte Rackspace.

  Tous les comptes Rackspace du nuage public sont définis par défaut au niveau de service Infrastructure gérée. Vous pouvez effectuer une mise à niveau vers le niveau de service Opérations gérées dans le

panneau de commande du nuage. En haut du panneau de commande du nuage, cliquez sur le nom d'utilisateur de votre compte, puis sélectionnez Upgrade Service Level (Mettre à niveau le niveau de service).

- Obtenez une licence pour l'ASA virtuel. Jusqu'à ce que vous obteniez une licence pour l'ASA virtuel, il fonctionnera en mode dégradé, ce qui n'autorisera que 100 connexions et un débit de 100 kbit/s. Consultez Gestion des licences pour l'ASA virtuel, à la page 1.
- Exigences d'interface :
  - Interface de gestion
  - Interfaces interne et externe
  - (Facultatif) Sous-réseau supplémentaire (DMZ)
- Chemins de communication :
  - Interface de gestion : utilisée pour connecter l'ASA virtuel à ASDM; ne peut pas être utilisée pour le trafic traversant.
  - Interface interne (requise) : utilisée pour connecter l'ASA virtuel aux hôtes internes.
  - Interface externe (requise) : utilisée pour connecter l'ASA virtuel au réseau public.
  - Interface DMZ (facultative) : utilisée pour connecter l'ASA virtuel au réseau DMZ.
- Pour la compatibilité des systèmes ASA et ASA virtuel et les exigences, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

Réseau Rackspace Cloud

Votre configuration en nuage peut inclure plusieurs types de réseaux, connectés selon vos besoins. Vous pouvez gérer les capacités de mise en réseau de vos serveurs en nuage de la même manière que vous gérez vos autres réseaux. Votre déploiement ASA virtuel interagira principalement avec trois types de réseaux virtuels dans Rackspace Cloud :

- PublicNet : connecte les composants de l'infrastructure en nuage, comme les serveurs en nuage, les équilibreurs de charges en nuage et les appareils réseau à Internet.
  - Utilisez PublicNet pour connecter l'ASA virtuel à Internet.
  - L'ASA virtuel s'associe à ce réseau par l'intermédiaire de l'interface Management0/0.
  - PublicNet est à double pile pour IPv4 et IPv6. Lorsque vous créez un serveur avec PublicNet, votre serveur reçoit une adresse IPv4 et une adresse IPv6 par défaut.
- ServiceNet : un réseau multilocataire interne uniquement IPv4 dans chaque région de Rackspace Cloud.
  - ServiceNet est optimisé pour acheminer le trafic entre les serveurs au sein de votre configuration (trafic est-ouest).
  - Il fournit aux serveurs un accès sans frais aux services régionalisés tels que les fichiers en nuage, les équilibreurs de charges en nuage, les bases de données en nuage et la sauvegarde en nuage.

- Les réseaux 10.176.0.0/12 et 10.208.0.0/12 sont réservés à ServiceNet. Tous les serveurs qui ont une connectivité ServiceNet recevront une adresse IP de l'un de ces réseaux.
- L'ASA virtuel se connecte à ce réseau par l'intermédiaire de l'interface Gigabit0/0.

- Réseaux en nuage privé : Cloud Networks (réseaux en nuage) vous permet de créer et de gérer des réseaux sécurisés et isolés dans le nuage.
  - Ces réseaux sont entièrement pour détenteur unique, et vous avez un contrôle total sur la topologie du réseau, l'adressage IP (IPv4 ou IPv6) et les serveurs en nuage qui sont associés.
  - Les réseaux en nuage ont une portée régionale et vous pouvez les associer à n'importe lequel de vos serveurs en nuage dans une région donnée.
  - Vous pouvez créer et gérer des réseaux en nuage par l'intermédiaire d'une API ou en utilisant le panneau de contrôle de Rackspace Cloud.

    L'ASA virtuel s'associe à ces réseaux par les interfaces Gigabit0/1 à Gigabit0/8.

Configuration Rackspace Day 0 (jour 0)

Lorsqu'une machine virtuelle est déployée dans Rackspace Cloud, un périphérique CD-ROM contenant des fichiers avec des informations de provisionnement Rackspace est connecté à la machine virtuelle. Les informations de provisionnement comprennent ce qui suit :

- Nom d'hôte
- Adresses IP pour les interfaces requises
- Routes IP statiques
- Nom d'utilisateur et mot de passe (clé publique SSH facultative)
- Serveurs DNS
- Serveurs NTP

Ces fichiers sont lus pendant le déploiement initial et la configuration ASA est générée.

Nom de domaine ASA virtuel

Par défaut, le nom de domaine ASA virtuel est le nom que vous attribuez à votre serveur en nuage lorsque vous commencez à créer votre ASA virtuel.

```
hostname rackspace-asav
```

La configuration du nom de domaine ASA n'acceptera qu'un nom de domaine conforme aux RFC 1034 et 1101 :

- Doit commencer et se terminer par une lettre ou un chiffre.
- Les caractères intérieurs doivent être une lettre, un chiffre ou un tiret.

Remarque L'ASA virtuel modifiera le nom du serveur en nuage pour se conformer à ces règles tout en le rendant aussi proche que possible du nom du serveur en nuage d'origine. Il supprimera les caractères spéciaux du début et de la fin du nom du serveur en nuage et remplacera les caractères intérieurs non conformes par un tiret.

Par exemple, un serveur en nuage nommé **ASAv-9.13.1.200** aura le nom de domaine **ASAv-9-13-1-200**.

Interfaces

Les interfaces sont configurées de la manière suivante :

- Management0/0
  - Nommée « outside » (externe) parce qu'elle est connectée au PublicNet.
  - Rackspace attribue des adresses publiques IPv4 et IPv6 à l'interface PublicNet.
- Gigabit0/0
  - Nommée « management » (gestion) parce qu'elle est connecté à ServiceNet.
  - Rackspace attribue une adresse IPv4 du sous-réseau ServiceNet pour la région Rackspace.
- De Gigabit0/1 à Gigabit0/8
  - Nommées « inside » (interne), « inside02 », « inside03 », etc., car elles sont connectées à des réseaux en nuage privés.
  - Rackspace attribue une adresse IP du sous-réseau du réseau en nuage.

La configuration d'interface pour un ASA virtuel avec 3 interfaces ressemblerait à ceci :

```
interface GigabitEthernet0/0
 nameif management
 security-level 0
 ip address 10.176.5.71 255.255.192.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.19.219.7 255.255.255.0
!
interface Management0/0
 nameif outside
 security-level 0
 ip address 162.209.103.109 255.255.255.0
 ipv6 address 2001:4802:7800:1:be76:4eff:fe20:1763/64
```

Routes statiques

Rackspace provisionne les routes IP statiques suivantes :

- Route IPv4 par défaut par le biais de l'interface PublicNet (**outside**) (externe).
- Route IPv6 par défaut par le biais de l'interface PublicNet.

- Routes de sous-réseau d'infrastructure sur l'interface ServiceNet (**management**) (gestion).

```
route outside 0.0.0.0 0.0.0.0 104.130.24.1 1
ipv6 route outside ::/0 fe80::def
route management 10.176.0.0 255.240.0.0 10.176.0.1 1
route management 10.208.0.0 255.240.0.0 10.176.0.1 1
```

Coordonnées de connexion

Un nom d'utilisateur « admin » est créé avec un mot de passe créé par Rackspace. Une clé publique pour l'utilisateur « admin » est créée si le serveur en nuage est déployé avec une clé publique pour Rackspace.

```
username admin password <admin_password> privilege 15
username admin attributes
 ssh authentication publickey <public_key>
```

La configuration SSH de Day0 (jour 0):

- SSH par le biais de l'interface PublicNet (**outside**) (externe) est activé pour IPv4 et IPv6.
- SSH par le biais de l'interface ServiceNet (**management**) (gestion), est activé pour IPv4.
- Configurer le groupe d'échange de clés renforcé à la demande de Rackspace.

```
aaa authentication ssh console LOCAL
ssh 0 0 management
ssh 0 0 outside
ssh ::0/0 outside
ssh version 2
ssh key-exchange group dh-group14-sha1
```

DNS et NTP

Rackspace fournit deux adresses de service IPv4 à utiliser pour DNS et NTP.

```
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 69.20.0.164
 name-server 69.20.0.196

ntp server 69.20.0.164
ntp server 69.20.0.196
```

Déployer l'ASA virtuel

Vous pouvez déployer l'ASA virtuel en tant qu'appliance virtuelle dans Rackspace Cloud. Cette procédure vous montre comment installer un périphérique à instance unique ASA virtuel .

Avant de commencer

Passez en revue la rubrique Configuration Rackspace Day 0 (jour 0), à la page 190 pour obtenir une description des paramètres de configuration que Rackspace Cloud active pour un déploiement ASA virtuel réussi, y compris les exigences de nom de domaine, le provisionnement d'interface et les informations sur le réseau.

Procédure

Étape 1 Sur le portail Rackspace mycloud, accédez à **SERVERS (serveurs)** > **CREATE RESOURCES (créer des ressources)** > **Cloud Server (serveur en nuage)**.

Étape 2 Dans la page **Create Server** (créer un serveur), saisissez les **détails de votre serveur** :

a) Saisissez le nom de votre machine ASA virtuel dans le champ **Server Name** (nom du serveur).

b) Sélectionnez votre région dans la liste déroulante **Region** (région).

Étape 3 Sous **Image**, choisissez **Linux/Appliances** > **ASAv** > **Version**.

Remarque
Vous choisirez généralement la version la plus récente prise en charge lors du déploiement d'un nouveau ASA virtuel.

Étape 4 Sous **Flavor**, choisissez une **Flavor Class** qui correspond à vos besoins en ressources; consultez Tableau 22 : Enveloppes prises en charge par Rackspace, à la page 187 pour obtenir la liste des machines virtuelles appropriées.

Important
À partir de la version 9.13(1), la mémoire minimale requise pour l'ASA virtuel est de 2 Go. Lors du déploiement d'un ASA virtuel avec plus de 1 vCPU, la mémoire minimale requise pour l'ASA virtuel est de 4 Go.

Étape 5 (Facultatif) Sous **Advanced Options**(options avancées), configurez une clé SSH.

Consultez Gestion de l'accès avec les clés SSH pour obtenir des renseignements complets sur les clés SSH dans Rackspace Cloud.

Étape 6 Passez en revue toutes les **Recommended Installs** (installations recommandées) et les **Itemized Charges** (frais détaillés) applicables pour votre ASA virtuel, puis cliquez sur **Create Server** (créer un serveur).

Le mot de passe de l'administrateur racine s'affiche. Copiez le mot de passe, puis ignorez la boîte de dialogue.

Étape 7 Après avoir créé le serveur, la page des détails du serveur s'affiche. Attendez que le serveur affiche un état actif. Cela prend quelques minutes.

Prochaine étape

- Connectez-vous au ASA virtuel.
- Poursuivez la configuration à l'aide des commandes CLI disponibles pour une entrée par le biais du protocole SSH ou utilisez ASDM. Consultez Démarrer ASDM pour obtenir des instructions concernant l'accès à ASDM.

Utilisation et rapport d'utilisation du processeur (CPU)

Le rapport sur l'utilisation du processeur résume le pourcentage du processeur utilisé pendant la période précisée. En règle générale, le cœur fonctionne sur environ 30 à 40 % de la capacité totale du processeur en dehors des heures de pointe et sur environ 60 à 70 % de capacité pendant les heures de pointe.

Utilisation de vCPU dans ASA virtuel

L'utilisation du vCPU 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 Rackspace comprend l'utilisation de l'ASA virtuel comme décrit plus :

- Délai d'inactivité d'ASA virtuel
- %SYS surdébit utilisé pour la machine 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

La commande **show cpu usage** (afficher l'utilisation du processeur) peut être utilisée pour afficher les statistiques d'utilisation du processeur.

Exemple

```
Ciscoasa#show cpu usage

Utilisation du processeur pendant 5 secondes = 1 %; 1 minute : 2 %; 5 minutes : 1 %
```

Voici un exemple dans lequel l'utilisation de vCPU signalée est sensiblement différente :

- Rapports ASA virtuel : 40 %
- DP : 35 %
- Processus externes : 5 %
- 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.

Rapport d'utilisation du processeur (CPU) de Rackspace

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 Rackspace

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et Rackspace :

- Les numéros de graphique Rackspace sont toujours supérieurs aux numéros de l'ASA virtuel.
- Rackspace 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 :

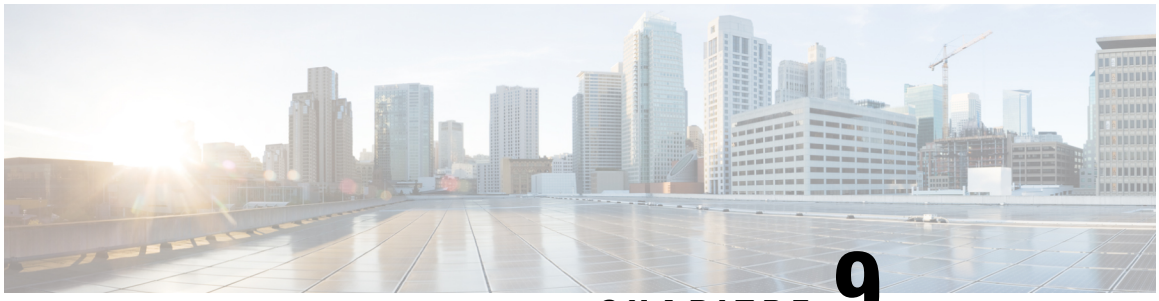
- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

Rackspace 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



CHAPITRE 9

Déployer l'ASA virtuel à l'aide d'Hyper-V

Vous pouvez déployer l'ASA virtuel à l'aide de Microsoft Hyper-V.

Important À partir de la version 9.13(1), la mémoire minimale requise pour l'ASA virtuel est de 2 Go. Si votre ASA virtuel actuel fonctionne avec moins de 2 Go de mémoire, vous ne pouvez pas effectuer de mise à niveau vers la version 9.13(1) à partir d'une version antérieure sans augmenter la mémoire de votre machine ASA virtuel. Vous pouvez également redéployer une nouvelle machine ASA virtuel avec la version 9.13(1).

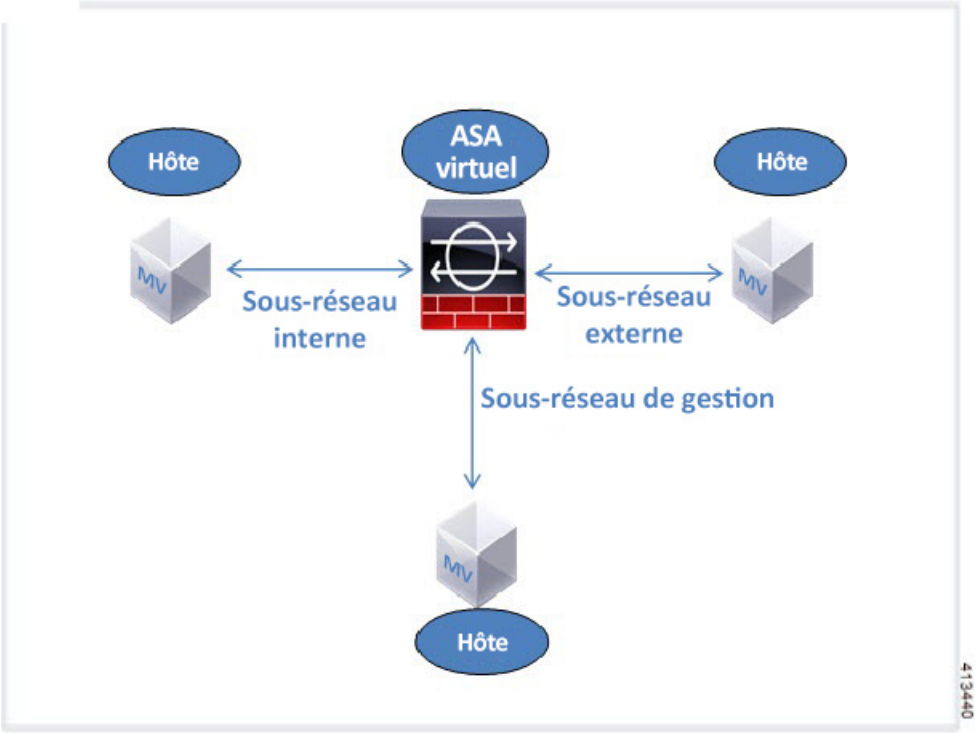
- Aperçu, à la page 197
- Lignes directrices et limites relatives à la licence, à la page 198
- Prérequis, à la page 199
- Préparer le fichier de configuration Day 0 (jour 0), à la page 200
- Déployer l'ASA virtuel avec le fichier de configuration Day 0 (jour 0) à l'aide du gestionnaire Hyper-V, à la page 202
- Déployer l'ASA virtuel sur Hyper-V à l'aide de la ligne de commande, à la page 203
- Déployer l'ASA virtuel sur Hyper-V à l'aide du gestionnaire Hyper-V, à la page 204
- Ajouter un adaptateur réseau à partir du gestionnaire Hyper-V, à la page 211
- Modifier le nom de l'adaptateur réseau, à la page 213
- Usurpation d'adresses MAC, à la page 214
- Configurer SSH, à la page 215
- Utilisation et rapport d'utilisation du processeur (CPU), à la page 215

Aperçu

Vous pouvez déployer Hyper-V sur un serveur Hyper-V autonome ou par l'intermédiaire du gestionnaire Hyper-V. Pour des instructions d'installation à l'aide des commandes d'interface de ligne de commande Powershell, consultez la section Installer l'ASA virtuel sur Hyper-V à l'aide de la ligne de commande, page 46. Pour des instructions d'installation à l'aide du gestionnaire Hyper-V, consultez Installer l'ASA virtuel sur Hyper-V à l'aide du gestionnaire Hyper-V, page 46. Hyper-V ne fournit pas d'option de console série. Vous pouvez gérer Hyper-V par le biais de SSH ou d'ASDM sur l'interface de gestion. Consultez la section Configuration de SSH à la page 54 pour obtenir plus de renseignements sur la configuration de SSH.

La figure suivante montre la topologie recommandée pour l'ASA virtuel en mode pare-feu routé. Trois sous-réseaux sont configurés dans Hyper-V pour l'ASA virtuel : gestion, interne et externe.

Illustration 37 : Topologie recommandée pour l'ASA virtuel en mode pare-feu routé



Lignes directrices et limites relatives à la licence

- Prise en charge des plateformes
  - Serveurs Cisco UCS, série B
  - Serveurs Cisco UCS, série C
  - Hewlett Packard Proliant DL160 Gen8
- Soutien pour le système d'exploitation
  - Windows Server 2019
  - Hyper-V natif

Remarque L'ASA virtuel devrait fonctionner sur la plupart des plateformes modernes (64 bits) et haute puissance utilisées pour la virtualisation.

- Format de fichier

  Prend en charge le format VHDX pour le déploiement initial de l'ASA virtuel sur Hyper-V.
- Configuration de Day 0 (jour 0)

Vous créez un fichier texte qui contient les commandes de configuration d'interface de ligne de commande ASA dont vous avez besoin. Consultez la section Préparer le fichier de configuration de Day 0 (jour 0) pour la procédure.

- Mode transparent du pare-feu avec la configuration de Day 0 (jour 0)

  La ligne de configuration « firewall transparent » (pare-feu transparent) doit être en haut du fichier de configuration de Day 0 (jour 0); si elle apparaît ailleurs dans le fichier, vous pourriez rencontrer un comportement erratique. Consultez la section Préparer le fichier de configuration de Day 0 (jour 0) pour la procédure.

- Basculement

  L'ASA virtuel sur Hyper-V prend en charge le basculement actif/veille. Pour le basculement actif/veille en mode avec routeur et en mode transparent, vous devez activer l'usurpation d'adresse MAC sur tous les adaptateurs de réseau virtuel. Consultez Configurer l'usurpation d'adresse MAC. Pour le mode transparent dans l'ASA virtuel, l'interface de gestion ne doit pas activer l'usurpation d'adresse MAC, car le basculement actif/veille n'est pas pris en charge.

- Hyper-V prend en charge jusqu'à huit interfaces. Management 0/0 et GigabitEthernet 0/0 jusqu'à 0/6. Vous pouvez utiliser GigabitEthernet comme liaison de basculement.

- Réseaux VLAN

  Utilisez la commande Hyper-V Powershell **Set-VMNetworkAdapterVLan** pour définir les VLAN sur une interface en mode de solutions de liaisons. Vous pouvez définir le NativeVlanID pour l'interface de gestion comme VLAN particulier ou « 0 » pour aucun VLAN. Le mode de liaison n'est pas persistant pendant les redémarrages de l'hôte Hyper-V. Vous devez reconfigurer le mode de liaison après chaque redémarrage.

- Les adaptateurs de réseau existants ne sont pas pris en charge.

- Les machines virtuelles de génération 2 ne sont pas prises en charge.

- Microsoft Azure n'est pas pris en charge.

Prérequis

- Installez Hyper-V sur MS Windows 2012.

- Créez le fichier texte de configuration de Day 0 (jour 0) si vous en utilisez un.

  Vous devez ajouter la configuration de Day 0 avant que l'ASA virtuel soit déployé pour la première fois; sinon, vous devez effectuer un effacement en écriture à partir d'ASA virtuel pour utiliser la configuration de Day 0. Consultez la section Préparer le fichier de configuration de Day 0 pour la procédure.

- Téléchargez le fichier ASA virtuel VHDX à partir de Cisco.com

  http://www.cisco.com/go/asa-software

Remarque Une connexion à Cisco.com et un contrat de service Cisco sont requis.

- Commutateur Hyper-V configuré avec au moins trois sous-réseaux/VLAN.

- Pour les exigences du système Hyper-V, consultez Compatibilité de Cisco Secure Firewall ASA.

Préparer le fichier de configuration Day 0 (jour 0)

Vous pouvez préparer un fichier de configuration de Day 0 (jour 0) avant de lancer l'ASA virtuel. Ce fichier est un fichier texte qui contient la configuration ASA virtuel qui sera appliquée lors du lancement d'ASA virtuel. Cette configuration initiale est placée dans un fichier texte nommé « day0-config » dans un répertoire de travail que vous avez choisi, puis manipulée dans un fichier day0.iso qui est monté et lu lors du premier démarrage. Au minimum, le fichier de configuration de Day 0 (jour 0) doit contenir des commandes qui activeront l'interface de gestion et configureront le serveur SSH pour l'authentification par clé publique, mais il peut également contenir une configuration ASA complète. Le fichier day0.iso (votre fichier day0.iso personnalisé ou le fichier day0.iso par défaut) doit être disponible lors du premier démarrage.

Avant de commencer

Nous utilisons Linux dans cet exemple, mais il existe des utilitaires similaires pour Windows.

- Pour autoriser automatiquement l'ASA virtuel lors du déploiement initial, placez le jeton d'identité de licence Smart (ID) que vous avez téléchargé à partir de Cisco Smart Software Manager dans un fichier texte nommé « idtoken » dans le même répertoire que le fichier de configuration de Day 0 (jour 0).
- Si vous souhaitez déployer l'ASA virtuel en mode transparent, vous devez utiliser un fichier de configuration ASA connu en cours d'exécution en mode transparent comme fichier de configuration de Day 0 (jour 0). Cela ne s'applique pas à un fichier de configuration de Day 0 (jour 0) pour un pare-feu avec routeur.
- Vous devez ajouter le fichier de configuration de Day 0 (jour 0) avant de démarrer l'ASA virtuel pour la première fois. Si vous décidez que vous souhaitez utiliser une configuration de Day 0 (jour 0) après avoir démarré l'ASA virtuel, vous devez exécuter une commande **write erase**, appliquer le fichier de configuration de Day 0 (jour 0), puis démarrer l'ASA virtuel.

Procédure

Étape 1 Saisissez la configuration CLI pour l'ASA virtuel dans un fichier texte appelé « day0-config ». Ajoutez des configurations d'interface pour les trois interfaces et toute autre configuration de votre choix.

La première ligne doit commencer par la version de l'ASA. La configuration day0-config doit être une configuration ASA valide. La meilleure façon de générer le fichier day0-config est de copier les parties souhaitées d'une configuration en cours d'exécution à partir d'un ASA ou d'ASA virtuel. L'ordre des lignes dans day0-config est important et doit correspondre à l'ordre observé dans une sortie de commande show run existante.

Exemple :

```
ASA Version 9.5.1
!
interface management0/0
nameif management
 security-level 100
 ip address 192.168.1.2 255.255.255.0
 no shutdown
interface gigabitethernet0/0
 nameif inside
```

```
 security-level 100
 ip address 10.1.1.2 255.255.255.0
 no shutdown
interface gigabitethernet0/1
 nameif outside
 security-level 0
 ip address 198.51.100.2 255.255.255.0
 no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
```

Étape 2 (Facultatif) Téléchargez le fichier de jeton d'identité de la licence Smart émis par Cisco Smart Software Manager sur votre ordinateur.

Étape 3 (Facultatif) Copiez le jeton d'identité à partir du fichier téléchargé et placez-le dans un fichier texte nommé qui contient uniquement le jeton d'identité.

Étape 4 (Facultatif) Pour l'octroi de licences automatisé lors du déploiement initial d'ASA virtuel, assurez-vous que les informations suivantes se trouvent dans le fichier day0-config :

- Adresse IP de l'interface de gestion
- (Facultatif) Proxy HTTP à utiliser pour les licences Smart
- Une commande de routeur qui active la connectivité au proxy HTTP (si précisé) ou à tools.cisco.com
- Un serveur DNS qui corrige tools.cisco.com en adresse IP
- La configuration de licence Smart précise la licence ASA virtuel que vous demandez
- (Facultatif) Un nom d'hôte unique pour que l'ASA virtuel soit plus facile à trouver dans CSSM

Étape 5 Générez le CD-ROM virtuel en convertissant le fichier texte en fichier ISO :

```
stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size (byptes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

Le jeton d'identité enregistre automatiquement l'ASA virtuel sur le serveur de licences Smart.

Étape 6 Répétez les étapes 1 à 5 pour créer des fichiers de configuration par défaut distincts avec les adresses IP appropriées pour chaque ASA virtuel que vous souhaitez déployer.

Déployer l'ASA virtuel avec le fichier de configuration Day 0 (jour 0) à l'aide du gestionnaire Hyper-V

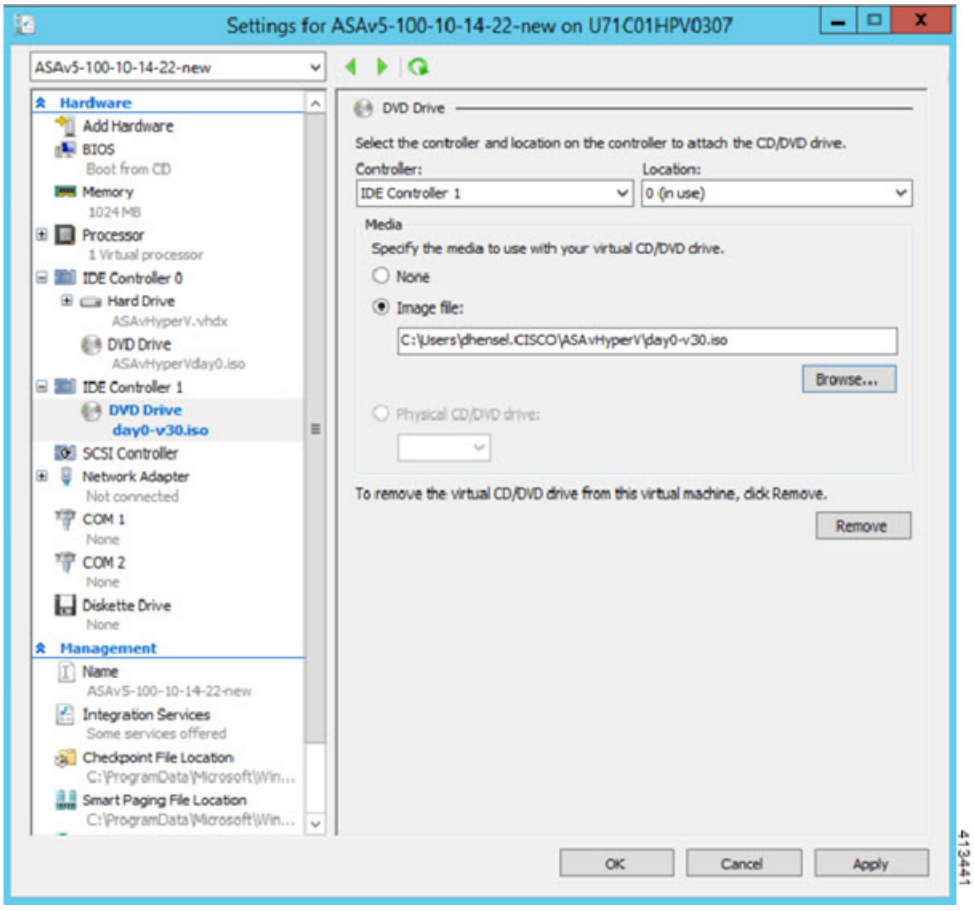
Après avoir configuré le fichier de configuration Day 0 (jour 0) (Prepare the Day 0 Configuration File (préparer le fichier de configuration Day 0)), vous pouvez le déployer à l'aide du gestionnaire Hyper-V.

Procédure

Étape 1 Accédez à **Server Manager (gestionnaire de serveur)** > **Tools (outils)** > **Hyper-V Manager (gestionnaire Hyper-V)**.

Étape 2 Cliquez sur **Settings** (paramètres) sur le côté droit du gestionnaire Hyper-V. La boîte de dialogue des paramètres s'ouvre. Sous **Hardware** (matériel) à gauche, cliquez sur **IDE Controller 1** (contrôleur IDE 1).

Illustration 38 : Gestionnaire Hyper-V



Étape 3 Sous **Media** (Médias) dans le volet droit, sélectionnez le bouton radio **Image file** (Fichier image), puis accédez au répertoire où vous conservez votre fichier de configuration ISO de Day 0 (jour 0), puis cliquez sur **Apply** (Appliquer).

Lorsque vous démarrez votre ASA virtuel pour la première fois, il sera configuré en fonction de ce qui se trouve dans le fichier de configuration de Day 0 (jour 0).

Déployer l'ASA virtuel sur Hyper-V à l'aide de la ligne de commande

Vous pouvez installer l'ASA virtuel sur Hyper-V à l'aide de la ligne de commande Windows Powershell. Si vous êtes sur un serveur Hyper-V autonome, vous devez utiliser la ligne de commande pour installer Hyper-V.

Procédure

Étape 1 Ouvrez un Windows PowerShell.

Étape 2 Déployer l'ASA virtuel :

Exemple :

```
new-vm -name $fullVMName -MemoryStartupBytes $memorysize -Generation 1 -vhdpath
C:\Users\jsmith.CISCO\ASAvHyperV\$ImageName.vhdx -Verbose
```

Étape 3 Selon votre modèle d'ASA virtuel, modifiez le nombre de CPU de la valeur par défaut de 1.

Exemple :

```
set-vm -Name $fullVMName -ProcessorCount 4
```

Étape 4 (Facultatif) Remplacez le nom de l'interface par quelque chose qui a du sens pour vous.

Exemple :

```
Get-VMNetworkAdapter -VMName $fullVMName -Name "Network Adapter" | Rename-vmNetworkAdapter -NewName
mgmt
```

Étape 5 (Facultatif) Modifiez l'ID du VLAN si votre réseau l'exige.

Exemple :

```
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1151 -Access -VMNetworkAdapterName "mgmt"
```

Étape 6 Actualisez l'interface pour que Hyper-V recueille les modifications.

Exemple :

```
Connect-VMNetworkAdapter -VMName $fullVMName -Name "mgmt" -SwitchName 1151mgmtswitch
```

Étape 7 Ajoutez l'interface interne.

Exemple :

```
Add-VMNetworkAdapter -VMName $fullVMName -name "inside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1552 -Access -VMNetworkAdapterName "inside"
```

Étape 8 Ajoutez l'interface externe.

Exemple :

```
Add-VMNetworkAdapter -VMName $fullVMName -name "outside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1553 -Access -VMNetworkAdapterName "outside"
```

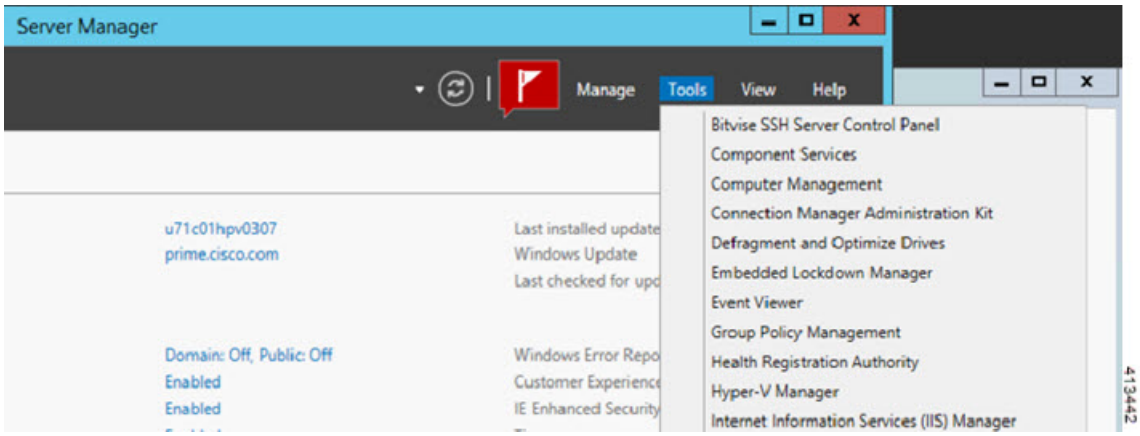
Déployer l'ASA virtuel sur Hyper-V à l'aide du gestionnaire Hyper-V

Vous pouvez utiliser le gestionnaire Hyper-V pour installer l'ASA virtuel sur Hyper-V.

Procédure

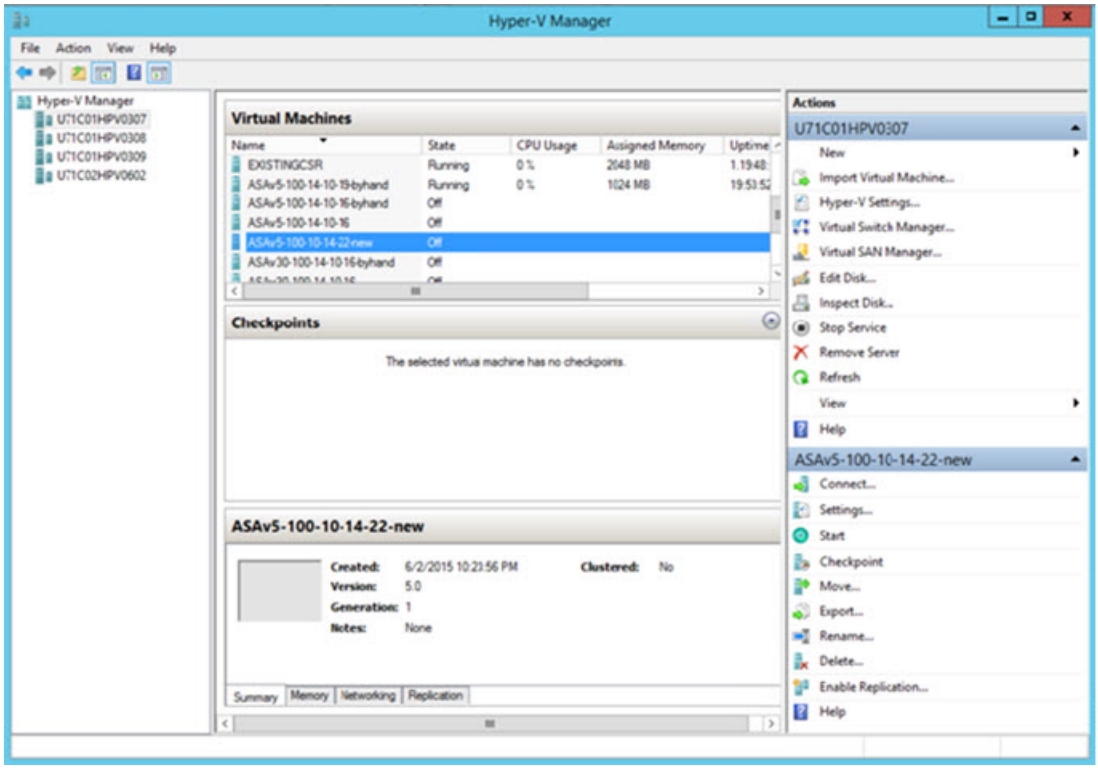
Étape 1 Accédez à **Server Manager (Gestionnaire de serveur)** > **Tools (Outils)** > **Hyper-V Manager (Gestionnaire Hyper-V)**.

Illustration 39 : Gestionnaire de serveur



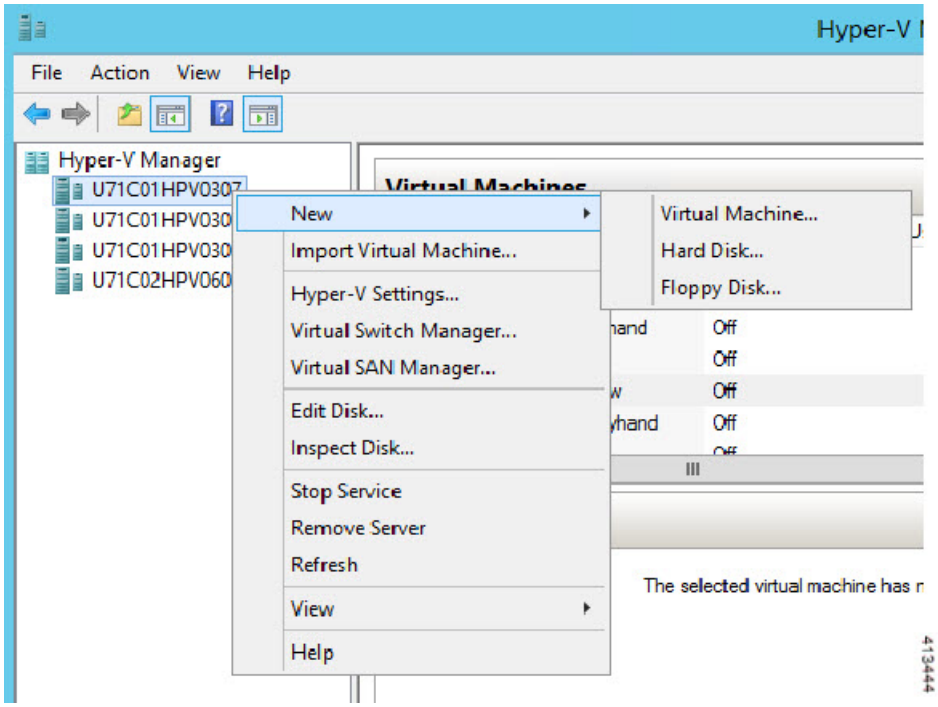
Étape 2 Le gestionnaire Hyper-V apparaît.

Illustration 40 : Gestionnaire Hyper-V



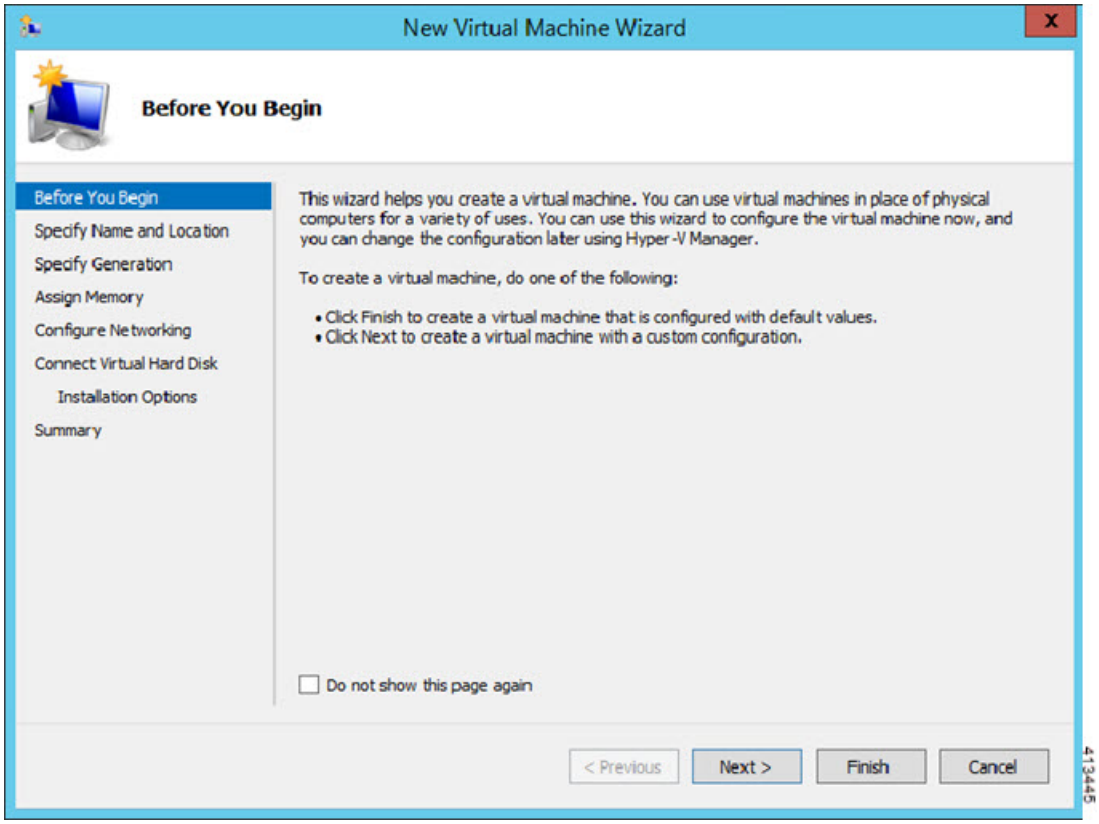
Étape 3 Dans la liste des hyperviseurs à droite, cliquez avec le bouton droit sur l'hyperviseur souhaité dans la liste et choisissez **New (Nouveau)** > **Virtual Machine (Machine virtuelle)**.

Illustration 41 : Lancer une nouvelle machine virtuelle



Étape 4 L'assistant de nouvelle machine virtuelle apparaît.

Illustration 42 : Assistant de nouvelle machine virtuelle



Étape 5 Par le biais de l'assistant, spécifiez les renseignements suivants :

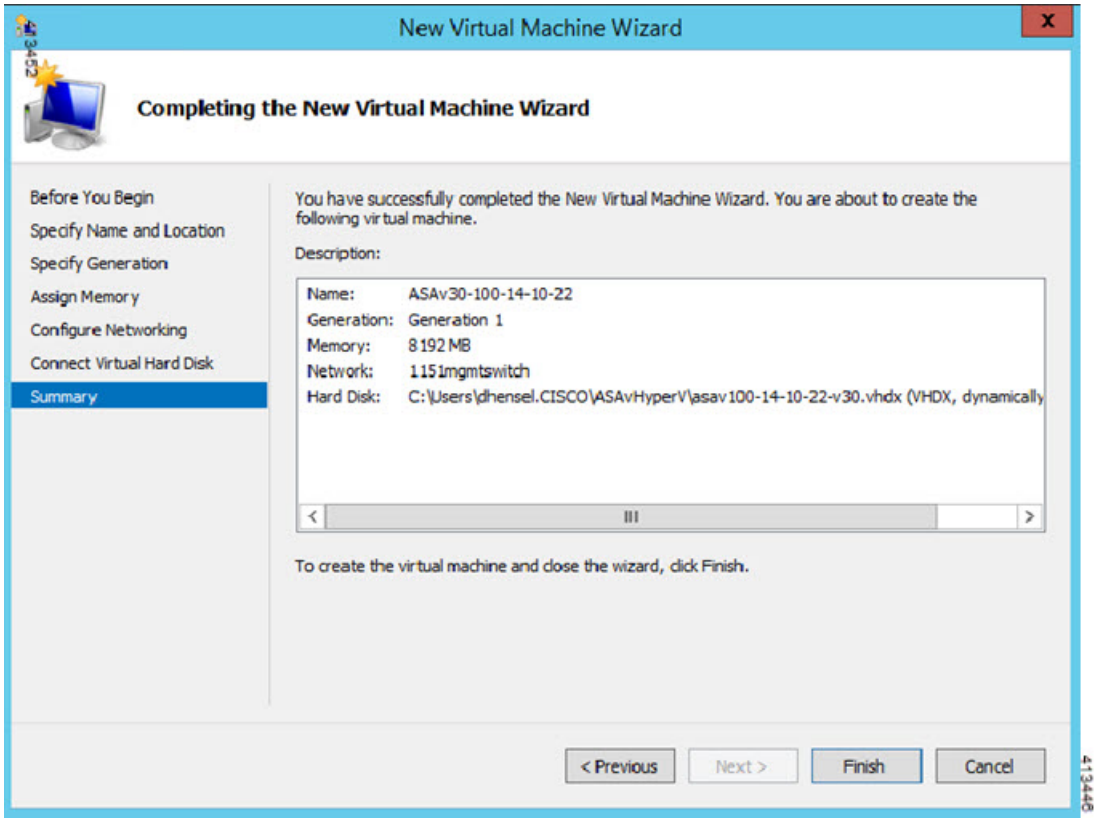
- Nom et emplacement de votre ASA virtuel
- Génération de votre ASA virtuel

  La seule génération prise en charge pour l'ASA virtuel est la **Génération 1**.
- Quantité de mémoire pour votre ASA virtuel (1 024 Mo pour 100 Mbit/s, 2 048 Mo pour 1 Gbit/s, 8 192 Mo pour 2 Gbit/s)
- Adaptateur réseau (connectez-vous au commutateur virtuel que vous avez déjà configuré)
- Disque dur virtuel et emplacement

  Choisissez **Use an existing virtual hard disk (Utiliser un disque dur virtuel existant)** et accédez à l'emplacement de votre fichier VHDX.

Étape 6 Cliquez sur Finish (Terminer) et une boîte de dialogue apparaît, indiquant votre configuration ASA virtuel.

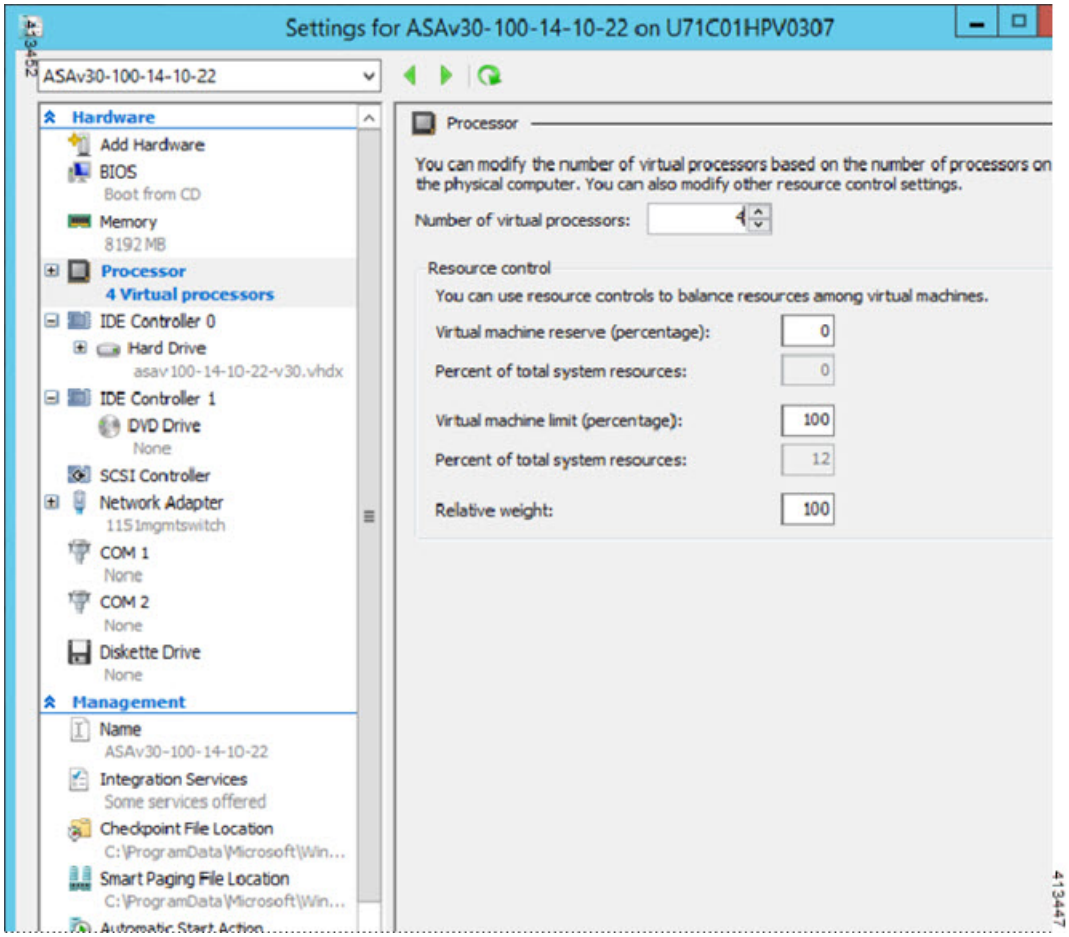
Illustration 43 : Résumé de la nouvelle machine virtuelle



Étape 7 Si votre ASA virtuel a quatre vCPU, vous devez modifier la valeur de vCPU avant de démarrer votre ASA virtuel. Cliquez sur **Settings** (Paramètres) sur le côté droit du gestionnaire Hyper-V. La boîte de dialogue des paramètres s'ouvre. Dans le menu Hardware (Matériel) à gauche, cliquez sur **Processor** (Processeur) pour accéder au volet Processor (Processeur). Modifiez le champ **Number of virtual processors** (Nombre de processeurs virtuels) à 4.

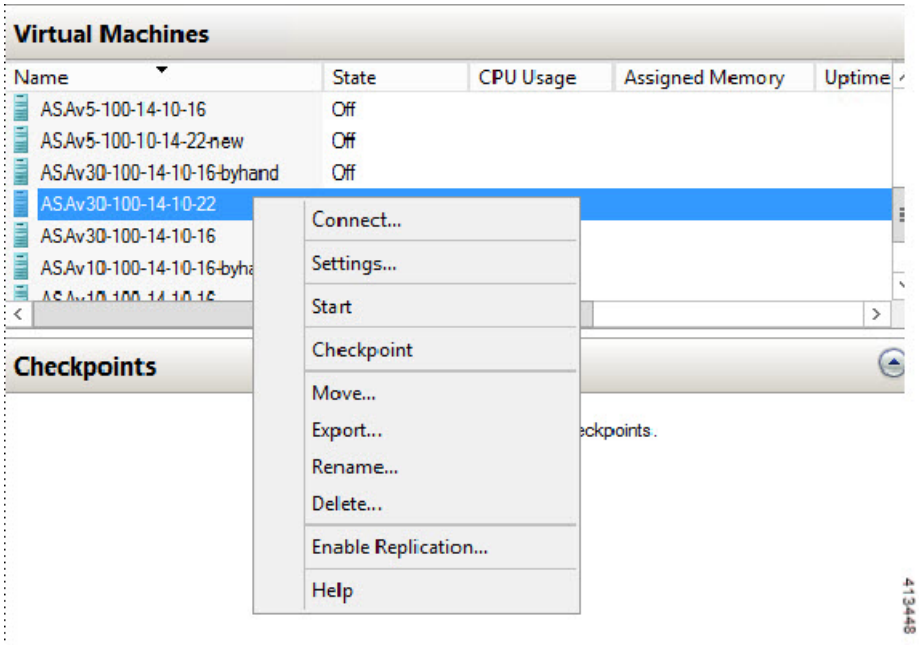
Les droits de 100 Mbit/s et de 1 Gbit/s ont un vCPU, et le droit de 2 Gbit/s a quatre vCPU. La valeur par défaut est 1.

Illustration 44 : Paramètres du processeur de la machine virtuelle



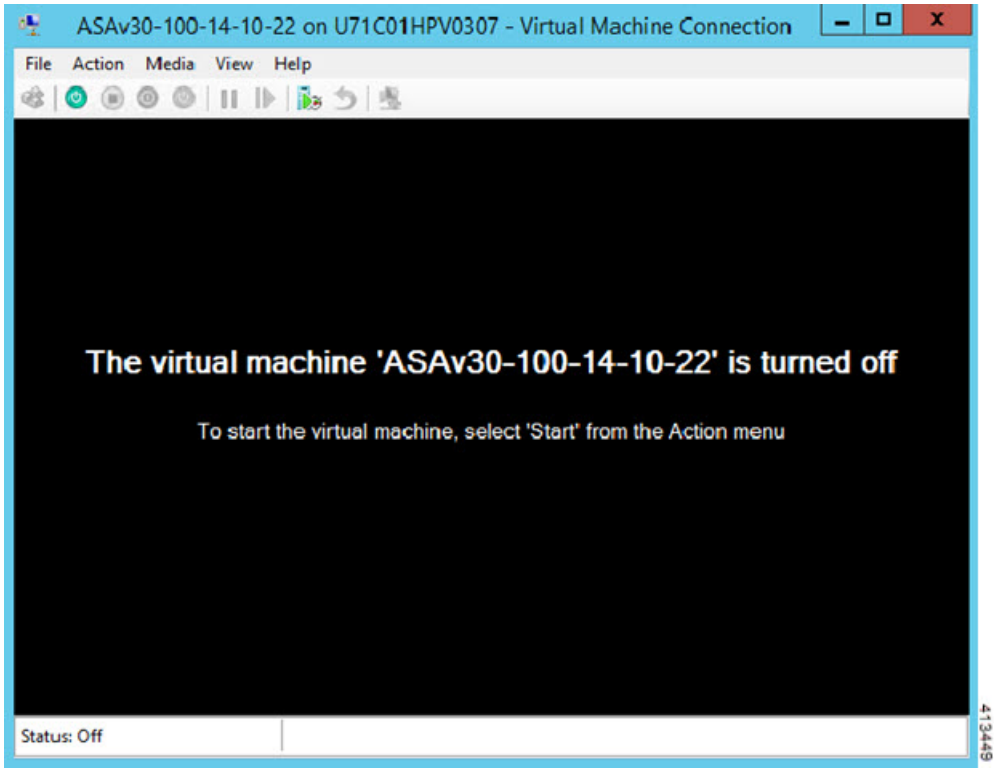
Étape 8 Dans le menu Virtual Machines (Machines virtuelles), connectez-vous à votre ASA virtuel en cliquant avec le bouton droit sur le nom de l'ASA virtuel dans la liste et en cliquant sur **Connect** (Connexion). La console s'ouvre avec l'ASA virtuel à l'arrêt.

Illustration 45 : Se connecter à la machine virtuelle



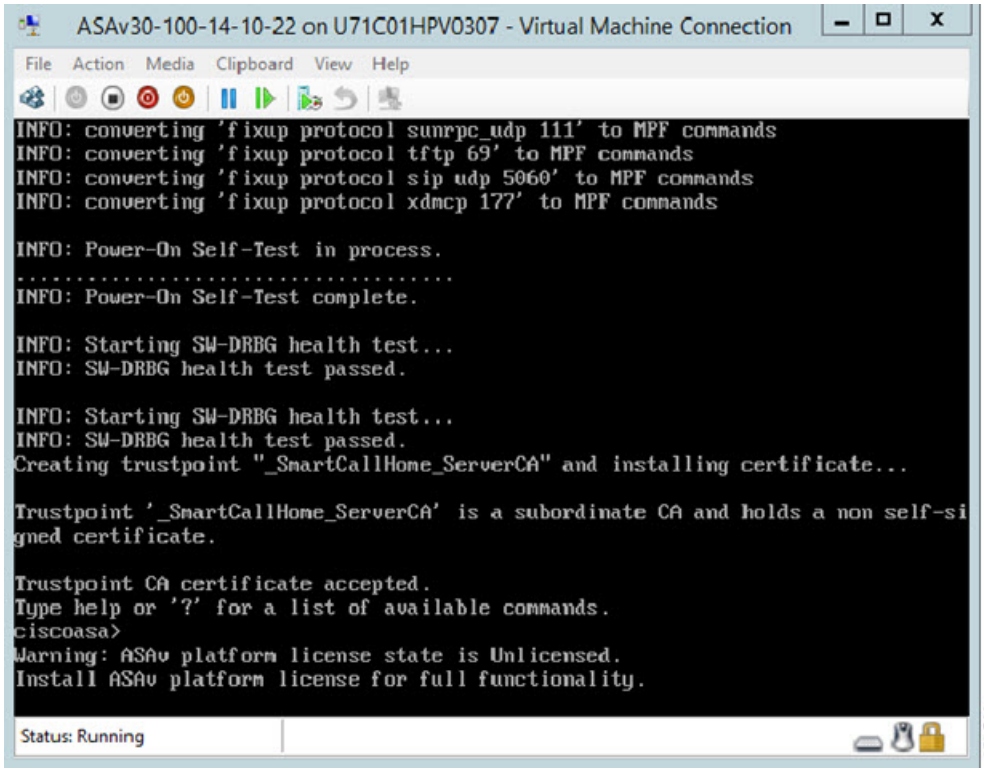
Étape 9 Dans la fenêtre de la console Virtual Machine Connection (Connexion de la machine virtuelle), cliquez sur le bouton turquoise de démarrage pour lancer l'ASA virtuel.

Illustration 46 : Démarrer la machine virtuelle



Étape 10 La progression du démarrage de l'ASA virtuel est affichée sur la console.

Illustration 47 : Progression du démarrage de la machine virtuelle



Ajouter un adaptateur réseau à partir du gestionnaire Hyper-V

Un ASA virtuel nouvellement déployé n'a qu'un seul adaptateur réseau. Vous devez ajouter au moins deux adaptateurs réseau supplémentaires. Dans cet exemple, nous ajoutons l'adaptateur réseau interne.

Avant de commencer

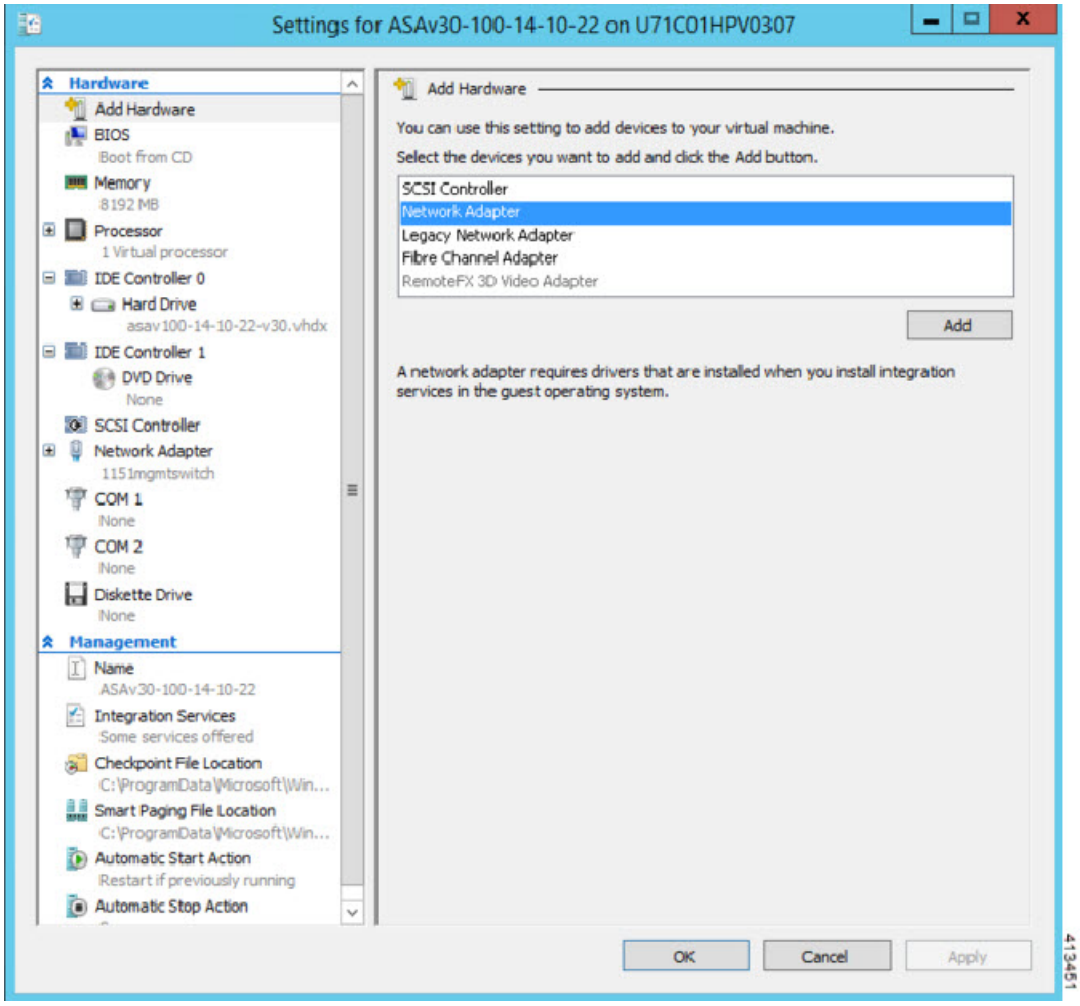
- L'ASA virtuel doit être à l'état désactivé.

Procédure

Étape 1 Cliquez sur **Settings** (Paramètres) sur le côté droit du gestionnaire Hyper-V. La boîte de dialogue des paramètres s'ouvre. Dans le menu Hardware (Matériel) à gauche, cliquez sur **Add Hardware** (Ajouter du matériel), puis sur **Network Adapter** (Adaptateur réseau).

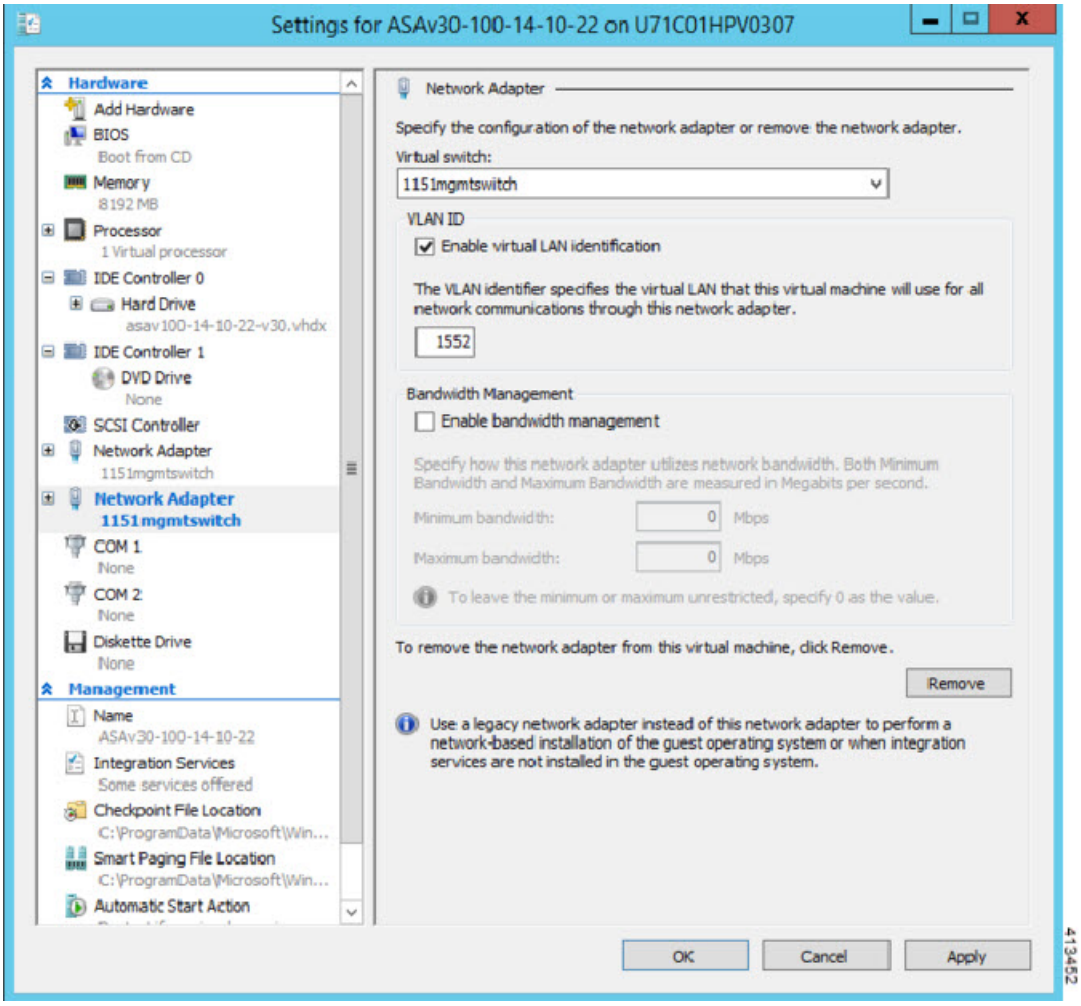
Remarque
N'utilisez PAS l'adaptateur réseau existant.

Illustration 48 : Ajouter un adaptateur réseau



Étape 2 Une fois l'adaptateur réseau ajouté, vous pouvez modifier le commutateur virtuel et d'autres fonctionnalités. Vous pouvez également définir l'ID du VLAN ici, au besoin.

Illustration 49 : Modifier les paramètres de l'adaptateur réseau



Modifier le nom de l'adaptateur réseau

Dans Hyper-V, un nom d'interface réseau générique est utilisé, « Network Adapter » (adaptateur réseau). Cela peut être source de confusion si les interfaces réseau ont toutes le même nom. Vous ne pouvez pas modifier le nom à l'aide du gestionnaire Hyper-V. Vous devez le modifier à l'aide des commandes Windows PowerShell.

Procédure

Étape 1 Ouvrez un Windows PowerShell.

Étape 2 Modifiez les adaptateurs réseau au besoin.

Exemple :

```
$NICRENAME= Get-VMNetworkAdapter -VMName 'ASAvVM' -Name "Network Adapter"
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[0] -newname inside
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[1] -newname outside
```

Usurpation d'adresses MAC

Pour que l'ASA virtuel transmette les paquets en mode transparent et pour le basculement HA Actif/Veille, vous devez activer l'usurpation d'adresses MAC pour TOUTES les interfaces. Vous pouvez le faire dans le gestionnaire Hyper-V ou en utilisant les commandes PowerShell.

Configurer l'usurpation d'adresse MAC à l'aide du gestionnaire Hyper-V

Vous pouvez utiliser le gestionnaire Hyper-V pour configurer l'usurpation d'adresse MAC sur Hyper-V.

Procédure

Étape 1 Accédez à **Server Manager (Gestionnaire de serveur)** > **Tools (Outils)** > **Hyper-V Manager (Gestionnaire Hyper-V)**.

Le gestionnaire Hyper-V apparaît.

Étape 2 Cliquez sur **Settings** (Paramètres) sur le côté droit du gestionnaire Hyper-V pour ouvrir la boîte de dialogue des paramètres.

Étape 3 Dans le menu **Hardware** (Matériel) à gauche :

1. Cliquez sur **Inside** (Interne) et développez le menu.
2. Cliquez sur **Advanced Functions** (Fonctions avancées) pour accéder à l'option d'adresse MAC.
3. Cliquez sur le bouton radio **Enable MAC address Spoofing** (Activer l'usurpation d'adresse MAC).

Étape 4 Répétez l'opération pour l'interface externe.

Configurer l'usurpation d'adresse MAC à l'aide de la ligne de commande

Vous pouvez utiliser la ligne de commande Windows Powershell pour configurer l'usurpation d'adresse MAC sur Hyper-V.

Procédure

Étape 1 Ouvrez un Windows PowerShell.

Étape 2 Configurez l'usurpation d'adresse MAC.

Exemple :

```
Set-VMNetworkAdapter -VMName $vm_name\
-ComputerName $computer_name -MacAddressSpoofing On\
-VMNetworkAdapterName $network_adapter\r"
```

Configurer SSH

Vous pouvez configurer l'ASA virtuel pour l'accès SSH sur l'interface de gestion à partir de la connexion de la machine virtuelle dans le gestionnaire Hyper-V. Si vous utilisez un fichier de configuration Day0 (Jour0), vous pouvez y ajouter un accès SSH. Consultez la section Préparer le fichier de configuration Day0 (Jour0) pour en savoir plus.

Procédure

Étape 1 Vérifiez que la paire de clés RSA est présente :

Exemple :

```
asav# show crypto key mypubkey rsa
```

Étape 2 S'il n'y a pas de paire de clés RSA, générez la paire de clés RSA :

Exemple :

```
asav(conf t)# crypto key generate rsa modulus 2048

username test password test123 privilege 15
aaa authentication ssh console LOCAL
ssh 10.7.24.0 255.255.255.0 management
ssh version 2
```

Étape 3 Vérifiez que vous pouvez accéder à l'ASA virtuel à partir d'un autre ordinateur à l'aide de SSH.

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 sur environ 30 à 40 % de la capacité totale du processeur en dehors des heures de pointe et sur environ 60 à 70 % de capacité pendant les heures de pointe.

Utilisation de vCPU dans l'ASA virtuel

L'utilisation de la vCPU 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 Hyper-V comprend l'utilisation de l'ASA virtuel comme décrit plus :

- Délai d'inactivité d'ASA virtuel

- %SYS surdébit utilisé pour la machine virtuelle ASA

Exemple d'utilisation du processeur

La commande **show cpu usage** (afficher l'utilisation du processeur) peut être utilisée pour afficher les statistiques d'utilisation du processeur.

Exemple

```
Ciscoasa#show cpu usage

Utilisation du processeur pendant 5 secondes = 1 %; 1 minute : 2 %; 5 minutes : 1 %
```

Voici un exemple dans lequel l'utilisation de vCPU signalée est sensiblement différente :

- Rapports ASA virtuel : 40 %
- DP : 35 %
- Processus externes : 5 %
- ASA (comme les rapports ASA virtuel) : 40 %
- Interrogation ASA inactive : 10 %
- Frais généraux : 45 %

CHAPITRE 10

Déployer l'ASA virtuel sur Oracle Cloud Infrastructure

Vous pouvez déployer l'ASA virtuel sur Oracle Cloud Infrastructure (OCI).

- Aperçu, à la page 217
- Prérequis, à la page 218
- Lignes directrices et limites relatives à la licence, à la page 218
- Exemple de topologie de réseau, à la page 220
- Déployer l'ASA virtuel , à la page 220
- Accéder à l'instance ASA virtuel sur OCI, à la page 226

Aperçu

OCI est un service informatique en nuage public qui vous permet d'exécuter vos applications dans un environnement hébergé hautement disponible offert par Oracle.

L'ASA virtuel exécute le même logiciel que les ASA virtuel physiques afin d'offrir des fonctionnalités de sécurité éprouvées dans un format virtuel. L'ASA virtuel peut être déployé dans l'OCI public. Il peut ensuite être configuré pour protéger les charges de travail des centres de données virtuels et physiques qui se développent, se contractent ou changent d'emplacement au fil du temps.

Formats de traitement OCI

Une forme est un modèle qui détermine le nombre de CPU, la quantité de mémoire et d'autres ressources qui sont allouées à une instance. L'ASA virtuel prend en charge les types de forme OCI *standard : à usage général* suivants :

Tableau 23 : Calculer les formes prises en charge pour ASA virtuel

Forme OCI	Version ASAv prise en charge	Attributs		Interfaces
		oCPU	RAM (Go)	
Intel VM.Standard 2.4	9.15, 9.16, 9.17, 9.18, 9.19, 9.20, 9.21 et 9.22 ou versions ultérieures	4	60	Minimum 4, Maximum 4

Forme OCI	Version ASAv prise en charge	Attributs		Interfaces
		oCPU	RAM (Go)	
IntelVM.Standard2.8	9.15, 9.16, 9.17, 9.18, 9.19, 9.20, 9.21 et 9.22 ou versions ultérieures	8	120	Minimum 4, Maximum 8

- L'ASA virtuel nécessite un minimum de 3 interfaces.
- Dans OCI, 1 oCPU équivaut à 2 vCPU.
- Le maximum de vCPU pris en charge est de 16 (8 oCPU).

Vous créez un compte sur OCI, lancez une instance de calcul à l'aide de l'offre de pare-feu virtuel Cisco ASA (ASA virtuel) sur le Marché Oracle Cloud et choisissez une forme OCI.

Prérequis

- Créez un compte sur https://www.oracle.com/cloud/sign-in.html.
- Obtenez une licence pour l'ASA virtuel. Jusqu'à ce que vous obteniez une licence pour l'ASA virtuel, il fonctionnera en mode dégradé, ce qui n'autorisera que 100 connexions et un débit de 100 kbit/s. Consultez Licences : gestion des licences Smart Software.
- Exigences d'interface :
  - Interface de gestion
  - Interfaces interne et externe
  - (Facultatif) Sous-réseau supplémentaire (DMZ)
- Chemins de communication :
  - Interface de gestion : utilisée pour connecter l'ASA virtuel à ASDM; ne peut pas être utilisée pour le trafic traversant.
  - Interface interne (requise) : utilisée pour connecter l'ASA virtuel aux hôtes internes.
  - Interface externe (requise) : utilisée pour connecter l'ASA virtuel au réseau public.
  - Interface DMZ (facultative) : utilisée pour connecter l'ASA virtuel au réseau DMZ.
- Pour les exigences du système ASA virtuel, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

L'ASA virtuel sur OCI prend en charge les fonctionnalités suivantes :

- Déploiement dans le réseau virtuel en nuage (VCN) OCI
- Maximum de 16 vCPU (8 oCPU) par instance
- Mode routé (par défaut)
- Licences : seul le protocole BYOL est pris en charge
- Prise en charge de la virtualisation des E/S à racine unique (SR-IOV)

Niveaux de performance pour Smart Licensing ASA virtuel

L'ASA virtuel prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement.

Niveau de performance	Type d'instance (cœur/RAM)	Limite du débit	Limite de session RA VPN
ASAv5	VM.Standard2.4 4 cœurs/60 Go	100 Mbit/sec	50
ASAv10	VM.Standard2.4 4 cœurs/60 Go	1 Gbit/sec	250
ASAv30	VM.Standard2.4 4 cœurs/60 Go	2 Gbit/s	750
ASAv50	VM.Standard2.8 8 cœurs/120 Go	S.O.	10 000
ASAv100	VM.Standard2.8 8 cœurs/120 Go	S.O.	20 000

Fonctionnalités non prises en charge

L'ASA virtuel sur OCI ne prend pas en charge les éléments suivants :

- Haute disponibilité en natif ASA virtuel
- Modes transparent/en ligne/passif
- Mode multi-contexte
- IPv6

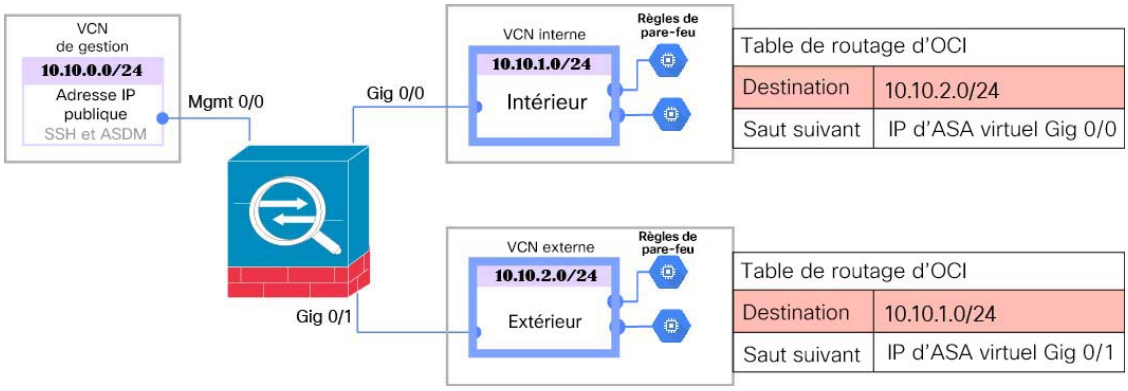
Restrictions

- Le déploiement d'ASA virtuel sur OCI ne prend pas en charge Mellanox 5 tant que vNIC en mode SR-IOV.
- Règles de routage distinctes requises pour la configuration d'ASAv statique et DHCP.

Exemple de topologie de réseau

La figure suivante montre la topologie de réseau recommandée pour l'ASA virtuel en mode pare-feu routé avec trois sous-réseaux configurés dans OCI pour l'ASA virtuel (gestion, interne et externe).

Illustration 50 : Exemple d'ASA virtuel sur le déploiement OCI



Déployer l'ASA virtuel

Les procédures suivantes décrivent comment préparer votre environnement OCI et lancer l'instance ASA virtuel. Vous vous connectez au portail OCI, recherchez dans le Marché OCI l'offre de pare-feu virtuel Cisco ASA (ASA virtuel) et lancez l'instance de calcul. Après avoir lancé l'ASA virtuel, vous devez configurer les tables de routage pour diriger le trafic vers le pare-feu en fonction de la source et de la destination du trafic.

Configurer le réseau virtuel en nuage (VCN)

Vous configurez le réseau en nuage virtuel (VCN) pour votre déploiement d'ASA virtuel. Au minimum, vous avez besoin de trois VCN, un pour chaque interface d'ASA virtuel.

Vous pouvez poursuivre les procédures suivantes pour terminer le VCN de gestion. Ensuite, vous revenez à **Networking** (Mise en réseau) pour créer des VCN pour les interfaces interne et externe.

Avant de commencer

Remarque Après avoir sélectionné un service dans le menu de navigation, le menu de gauche comprend la liste des compartiments. Les compartiments vous aident à organiser des ressources pour faciliter le contrôle d'accès. Votre compartiment racine est créé pour vous par Oracle lorsque votre location est provisionnée. Un administrateur peut créer d'autres compartiments dans le compartiment racine, puis ajouter les règles d'accès pour contrôler quels utilisateurs peuvent voir et agir en leur nom. Consultez le document Oracle « Gestion des compartiments » pour en savoir plus.

Procédure

Étape 1 Connectez-vous à OCI et choisissez votre région.

OCI est divisé en plusieurs régions isolées les unes des autres. La région est affichée dans le coin supérieur droit de votre écran. Les ressources d'une région n'apparaissent pas dans une autre région. Vérifiez périodiquement que vous êtes dans la région prévue.

Étape 2 Sélectionnez **Networking (Mise en réseau)** > **Virtual Cloud Networks (Réseaux de nuage virtuel)** et cliquez sur Create Virtual Cloud Networks (Créer des réseaux de nuage virtuel).

Étape 3 Saisissez un **Name** (Nom) descriptif pour votre réseau VCN, par exemple *ASAvManagement*.

Étape 4 Saisissez un **CIDR block** (Bloc CIDR) pour votre VCN.

Étape 5 Cliquez sur **Create VCN** (Créer un VCN).

Créer le groupe de sécurité réseau

Un groupe de sécurité réseau se compose d'un ensemble de vNIC et d'un ensemble de règles de sécurité qui s'appliquent à ces vNIC.

Procédure

Étape 1 Sélectionnez **Networking (Mise en réseau)** > **Virtual Cloud Networks (Réseaux virtuels en nuage)** > **Virtual Cloud Network Details (Détails du réseau virtuel en nuage)** > **Network Security Groups (Groupes de sécurité réseau)** et cliquez sur **Create Network Security Group** (Créer un groupe de sécurité réseau).

Étape 2 Saisissez un **Name** (Nom) de description pour votre groupe de sécurité réseau, par exemple *ASAv-Mgmt-Allow-22-443*.

Étape 3 Cliquez sur **Next** (suivant).

Étape 4 Ajoutez vos règles de sécurité :

a) Ajoutez une règle pour autoriser le port TCP 22 pour l'accès SSH à la console ASA virtuel.

b) Ajoutez une règle pour autoriser le port TCP 443 pour l'accès HTTPS à ASDM.

L'ASA virtuel peut être géré par ASDM, ce qui nécessite l'ouverture du port 443 pour les connexions HTTPS.

Étape 5 Cliquez sur **Create** (créer).

Créer la passerelle Internet

Une passerelle Internet est requise pour rendre votre sous-réseau de gestion accessible au public.

Procédure

Étape 1 Sélectionnez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails de réseau virtuel en nuage)** > **Internet Gateways (passerelles Internet)** et cliquez sur **Create Internet Gateway (créer une passerelle Internet)**.

Étape 2 Saisissez un **nom** descriptif pour votre passerelle Internet, par exemple, *ASAv-IG*.

Étape 3 Cliquez sur **Create Internet Gateway** (créer une passerelle Internet).

Étape 4 Ajouter le routeur à la passerelle Internet :

a) Choisissez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails du réseau virtuel en nuage)** > **Route Tables (tableaux de routage)**.
b) Cliquez sur le lien de votre tableau de routage par défaut pour ajouter des règles de routage.
c) Cliquez sur **Add Route Rules** (ajouter des règles de routage).
d) Dans la liste déroulante **Target Type** (type de cible), sélectionnez **Internet Gateway** (passerelle Internet).
e) Saisissez le bloc CIDR de l'IPv4 de destination, par exemple 0.0.0.0/0.
f) Dans la liste déroulante **Target Internet Gateway** (passerelle Internet cible), sélectionnez la passerelle que vous avez créée.
g) Cliquez sur **Add Route Rules** (ajouter des règles de routage).

Créer le sous-réseau

Chaque VCN aura au moins un sous-réseau. Vous créerez un sous-réseau de gestion pour le VCN de gestion. Vous aurez également besoin d'un sous-réseau interne pour le VCN interne et d'un sous-réseau externe pour le VCN externe.

Procédure

Étape 1 Sélectionnez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails du réseau virtuel en nuage)** > **Subnets (sous-réseaux)** et cliquez sur **Create Subnet (créer un sous-réseau)**.

Étape 2 Saisissez un **nom** descriptif pour votre sous-réseau, par exemple, *Gestion*.

Étape 3 Sélectionnez un **type de sous-réseau** (conservez la valeur par défaut recommandée de **Regional** (régional)).

Étape 4 Saisissez un **CIDR Block** (bloc CIDR), par exemple 10.10.0.0/24. L'adresse IP interne (non publique) du sous-réseau est extraite de ce bloc CIDR.

Étape 5 Sélectionnez l'un des tableaux de routage que vous avez créés précédemment dans la liste déroulante **Route Table** (tableau de routage).

Étape 6 Sélectionnez **Subnet Access** (accès au sous-réseau) pour votre sous-réseau.

Pour le sous-réseau de gestion, il doit s'agir de **Public Subnet** (sous-réseau public).

Étape 7 Sélectionnez **DHCP Option** (option DHCP).

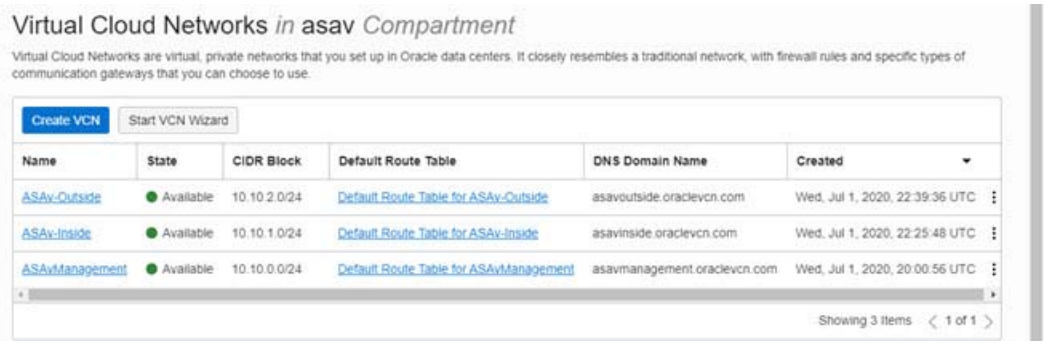
Étape 8 Sélectionnez une **Security List** (liste de sécurité) que vous avez créée précédemment.

Étape 9 Cliquez sur **Create Subnet** (créer un sous-réseau).

Prochaine étape

Après avoir configuré vos VCN (Gestion, Interne, Externe), vous pouvez lancer l'ASA virtuel. Consultez le schéma suivant pour un exemple de configuration VCN d'ASA virtuel.

Illustration 51 : Réseaux en nuage ASA virtuel



Créer l'instance ASA virtuel sur OCI

Vous déployez l'ASA virtuel sur OCI par l'intermédiaire d'une instance de traitement en utilisant l'offre de pare-feu virtuel Cisco ASA (ASA virtuel) sur le Marché Oracle Cloud. Vous sélectionnez la forme de machine la plus appropriée en fonction de caractéristiques telles que le nombre de CPU, la quantité de mémoire et les ressources du réseau.

Procédure

Étape 1 Connectez-vous au portail OCI.

La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.

Étape 2 Choisissez **Marketplace (Marché)** > **Applications**.

Étape 3 Effectuez une recherche sur le Marché pour « Cisco ASA virtual firewall (ASAv) » (Pare-feu virtuel Cisco ASA (ASAv)) et choisissez l'offre.

Étape 4 Passez en revue les conditions générales et cochez la case **I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.** (J'ai lu et j'accepte les conditions d'utilisation d'Oracle et les conditions générales des partenaires).

Étape 5 Cliquez sur **Launch Instance** (Lancer l'instance).

Étape 6 Saisissez un **Name** (Nom) descriptif pour votre instance, par exemple, *ASAv-9-15*.

Étape 7 Cliquez sur **Change Shape** (Modifier la forme) et sélectionnez la forme avec le nombre d'oCPU, la quantité de RAM et le nombre d'interfaces requises pour l'ASA virtuel; par exemple, VM.Standard2.4 (voir Tableau 23 : Calculer les formes prises en charge pour ASA virtuel, à la page 217).

Étape 8 Dans la liste déroulante **Virtual Cloud Network** (Réseau en nuage virtuel), choisissez le VCN de gestion.

Étape 9 Dans la liste déroulante **Subnet** (Sous-réseau), choisissez le sous-réseau de gestion s'il n'est pas rempli automatiquement.

Étape 10 Cochez la case **Use Network Security Groups to Control Traffic** (Utiliser les groupes de sécurité réseau pour contrôler le trafic) et choisissez le groupe de sécurité que vous avez configuré pour le VCN de gestion.

Étape 11 Cliquez sur le bouton radio **Assign a Public Ip Address** (Affecter une adresse IP publique).

Étape 12 Sous **Add SSH Keys** (Ajouter des clés SSH), cliquez sur le bouton radio **Paste Public Keys** (Coller des clés publiques) et collez la clé SSH.

Les instances basées sur Linux utilisent une paire de clés SSH au lieu d'un mot de passe pour authentifier les utilisateurs distants. Une paire de clés est composée d'une clé privée et d'une clé publique. Vous conservez la clé privée sur votre ordinateur et fournissez la clé publique lorsque vous créez une instance. Consultez la section Gestion des paires de clés sur les instances Linux pour obtenir des instructions.

Étape 13 Cliquez sur le lien **Show Advanced Options** (Afficher les options avancées) pour développer les options.

Étape 14 (Facultatif) Sous **Initialization Script** (Script d'initialisation), cliquez sur le bouton radio **Paste Cloud-Init Script** (Coller le script d'initialisation en nuage) pour fournir une configuration day0 (jour0) pour l'ASA virtuel. La configuration day0 (jour0) est appliquée lorsque l'ASA virtuel est lancé.

L'exemple suivant montre une configuration day0 (jour0) que vous pouvez copier et coller dans le champ **Cloud-Init Script** (Script d'initialisation en nuage) :

Consultez les Guides de configuration ASA et la Référence sur les commandes ASA pour en savoir plus sur les commandes ASA.

Important
Lorsque vous copiez du texte à partir de cet exemple, vous devez valider le script dans un éditeur de texte ou un moteur de validation tiers pour éviter les erreurs de format et supprimer les caractères Unicode non valides.

```
!ASA Version 9.18.1
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 60
ssh version 2
username admin nopassword privilege 15
username admin attributes
service-type admin
http server enable
http 0 0 management
aaa authentication ssh console LOCAL
```

Étape 15 Cliquez sur **Create** (créer).

Prochaine étape

Surveillez l'instance ASA virtuel, qui indique l'état Provisioning (Provisionnement) après avoir cliqué sur le bouton **Create** (Créer).

Important Il est important de surveiller l'état. Dès que l'instance ASA virtuel passe de l'état Provisioning (provisionnement) à l'état Running (En cours d'exécution), vous devez associer les VNIC comme nécessaire avant la fin du démarrage de l'ASA virtuel.

Associer les interfaces

L'ASA virtuel passe à l'état en cours d'exécution avec une VNIC associée (consultez **Compute (calculer)** > **Instances** > **Instance Details (détails de l'instance)** > **Attached VNICs (VNIC associées)**). C'est ce que l'on appelle la VNIC principale, et mappe au VCN de gestion. Avant que l'ASA virtuel ne termine le premier démarrage, vous devez associer les VNIC pour les autres sous-réseaux VCN que vous avez créés précédemment (à l'intérieur, à l'extérieur) afin que les VNIC soient correctement détectées sur ASA virtuel.

Procédure

Étape 1 Sélectionnez votre nouvelle instance ASA virtuel.

Étape 2 Choisissez **Attached VNICs (VNIC associées)** > **Create VNIC (créer une VNIC)**.

Étape 3 Saisissez un **nom** descriptif pour votre VNIC, par exemple *Inside* (intérieur).

Étape 4 Sélectionnez le VCN dans la liste déroulante **Virtual Cloud Network** (réseau virtuel en nuage).

Étape 5 Sélectionnez votre sous-réseau dans le menu déroulant **Subnet** (sous-réseau).

Étape 6 Cochez la case **Use Network Security Groups to Control Traffic (utiliser les groupes de sécurité réseau pour contrôler le trafic)** et choisissez le groupe de sécurité que vous avez configuré pour le VCN sélectionné.

Étape 7 Cochez la case **Skip Source Destination Check** (ignorer la vérification de la source de la destination) groupes de sécurité réseau pour contrôler le trafic.

Étape 8 (Facultatif) Précisez une **Private IP Address** (adresse IP privée). C'est obligatoire uniquement si vous souhaitez choisir une adresse IP particulière pour la VNIC.

Si vous ne spécifiez pas d'adresse IP, le protocole OCI attribuera une adresse IP du bloc CIDR que vous avez attribué au sous-réseau.

Étape 9 Cliquez sur **Save Changes** (enregistrer les modifications) pour créer la carte VNIC.

Étape 10 Répétez cette procédure pour chaque VNIC requise par votre déploiement.

Ajouter des règles de routage pour les VNIC associées

Ajoutez des règles de tableau de routage aux tableaux de routage interne et externe.

Procédure

Étape 1 Choisissez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > et cliquez sur le tableau de routage par défaut associé au VCN (interne ou externe).

Étape 2 Cliquez sur **Add Route Rules** (ajouter des règles de routage).

Étape 3 Dans la liste déroulante **Target Type** (type de cible), sélectionnez **Private IP** (adresse IP privée).

Étape 4 Dans la liste déroulante **Destination Type** (type de destination), sélectionnez **CIDR Block** (bloc CIDR).

Étape 5 Saisissez le **bloc CIDR de l'IPv4 de destination**, par exemple, 0.0.0.0/0.

Étape 6 Saisissez l'adresse IP privée de la VNIC dans le champ **Target Selection** (sélection de cible).

Si vous n'avez pas explicitement attribué d'adresse IP à la VNIC, vous pouvez trouver l'adresse IP attribuée automatiquement à partir des détails de la VNIC (**Compute (calcul)** > **Instances** > **Instance Details (détails de l'instance)** > **Attached VNICs (VNIC associées)**).

Étape 7 Cliquez sur **Add Route Rules** (ajouter des règles de routage).

Étape 8 Répétez cette procédure pour chaque VNIC requise par votre déploiement.

Remarque
Règles de routage distinctes requises pour la configuration d'ASA virtuel (statique et DHCP).

Accéder à l'instance ASA virtuel sur OCI

Vous pouvez vous connecter à une instance en cours d'exécution en utilisant une connexion Secure Shell (SSH).

- La plupart des systèmes de type UNIX incluent un client SSH par défaut.
- Les systèmes Windows 10 et Windows Server 2019 doivent inclure le client OpenSSH, dont vous aurez besoin si vous avez créé votre instance à l'aide des clés SSH générées par Oracle Cloud Infrastructure.
- Pour les autres versions de Windows, vous pouvez télécharger PuTTY, le client SSH gratuit depuis http://www.putty.org.

Prérequis

Vous aurez besoin des renseignements suivants pour vous connecter à l'instance :

- L'adresse IP publique de l'instance. Vous pouvez obtenir l'adresse à partir de la page Instance Details (Détails de l'instance) dans la console. Ouvrez le menu de navigation. Sous **Core Infrastructure** (Infrastructure principale), accédez à **Compute** (Informatique) et cliquez sur **Instances**. Ensuite, sélectionnez votre instance. Vous pouvez également utiliser les opérations ListVnicAttachments et GetVnic de l'API de services principaux.
- Le nom d'utilisateur et le mot de passe de votre instance.

- Le chemin complet vers la partie clé privée de la paire de clés SSH que vous avez utilisée lors du lancement de l'instance. Pour en savoir plus sur les paires de clés, consultez Gestion des paires de clés sur les instances Linux.

Remarque Vous pouvez vous connecter à l'instance ASA virtuel en utilisant les renseignements d'authentification spécifiés dans la configuration day0 (jour0) ou en utilisant la paire de clés SSH que vous avez créée lors du lancement de l'instance.

Se connecter à l'instance ASA virtuel à l'aide de SSH

Pour vous connecter à l'instance ASA virtuel à partir d'un système de type Unix, connectez-vous à l'instance à l'aide de SSH.

Procédure

Étape 1 Utilisez la commande suivante pour définir les autorisations de fichier afin que seul vous puissiez lire le fichier :

```
$ chmod 400 <private_key>
```

Lieu :

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

Étape 2 Utilisez la commande SSH suivante pour accéder à l'instance.

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

Lieu :

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

`<username>` correspond au nom d'utilisateur pour l'instance ASA virtuel.

`<public-ip-address>` correspond à l'adresse IP publique de votre instance que vous avez extraite de la console.

Se connecter à l'instance ASA virtuel à l'aide d'OpenSSH

Pour vous connecter à l'instance ASA virtuel à partir d'un système Windows, connectez-vous à l'instance à l'aide d'OpenSSH.

Procédure

Étape 1 Si c'est la première fois que vous utilisez cette paire de clés, vous devez définir les autorisations de fichier de sorte que vous puissiez être le seul à lire le fichier.

Procédez comme suit :

a) Dans Windows Explorer, accédez au fichier de clé privée, cliquez avec le bouton droit sur le fichier, puis cliquez sur **Properties** (Propriétés).
b) Dans l'onglet **Security** (Sécurité), cliquez sur **Advanced** (Avancé).
c) Assurez-vous que le **Owner** (Propriétaire) est votre compte d'utilisateur.
d) Cliquez sur **Disable Inheritance** (Désactiver l'hérédité), puis sélectionnez **Convert inherited permissions into explicit permissions on this object** (Convertir les autorisations héritées en autorisations explicites sur cet objet).
e) Sélectionnez chaque entrée d'autorisation qui ne correspond pas à votre compte d'utilisateur et cliquez sur **Remove** (Supprimer).
f) Assurez-vous que l'autorisation d'accès pour votre compte d'utilisateur est **Full control** (Contrôle complet).
g) Enregistrez vos modifications.

Étape 2 Pour vous connecter à l'instance, ouvrez Windows PowerShell et exécutez la commande suivante :

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

Lieu :

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

`<username>` correspond au nom d'utilisateur pour l'instance ASA virtuel.

`<public-ip-address>` correspond à l'adresse IP publique de votre instance que vous avez extraite de la console.

Se connecter à l'instance ASA virtuel à l'aide de PuTTY

Pour vous connecter à l'instance ASA virtuel à partir d'un système Windows à l'aide de PuTTY :

Procédure

Étape 1 Ouvrez PuTTY.

Étape 2 Dans le volet **Category (catégorie)**, sélectionnez **Session (session)** et saisissez la commande suivante :

- **Host Name (or IP address) (nom d'hôte ou adresse IP non valide)** :

  `<username>@<public-ip-address>`

  Lieu :

  `<username>` correspond au nom d'utilisateur pour l'instance ASA virtuel.

  `<public-ip-address>` correspond à votre adresse IP publique d'instance que vous avez extraite de la console.

- **Port:** 22
- **Connection type:** SSH

Étape 3 Dans le volet **Category** (Catégorie), développez **Window** (Fenêtre), puis sélectionnez **Translation** (Traduction).

Étape 4 Dans la liste déroulante **Remote character set** (Jeu de caractères du système distant), sélectionnez **UTF-8**.

Sur les instances basées sur Linux, les paramètres régionaux par défaut sont définis pour UTF-8. PuTTY est configuré pour utiliser les mêmes paramètres régionaux.

Étape 5 Dans le volet **Category** (Catégorie), développez la section **Connection** (Connexion), puis la section **SSH**. Cliquez ensuite sur **Auth** (Authentification).

Étape 6 Cliquez sur **Browse** (Parcourir), puis sélectionnez votre clé privée.

Étape 7 Cliquez sur **Open** (Ouvrir) pour démarrer la session.

S'il s'agit de votre première connexion à l'instance, un message indiquant que la clé d'hôte du serveur n'est pas mise en cache dans le registre pourrait s'afficher. Cliquez sur **Yes** (Oui) pour poursuivre.

CHAPITRE 11

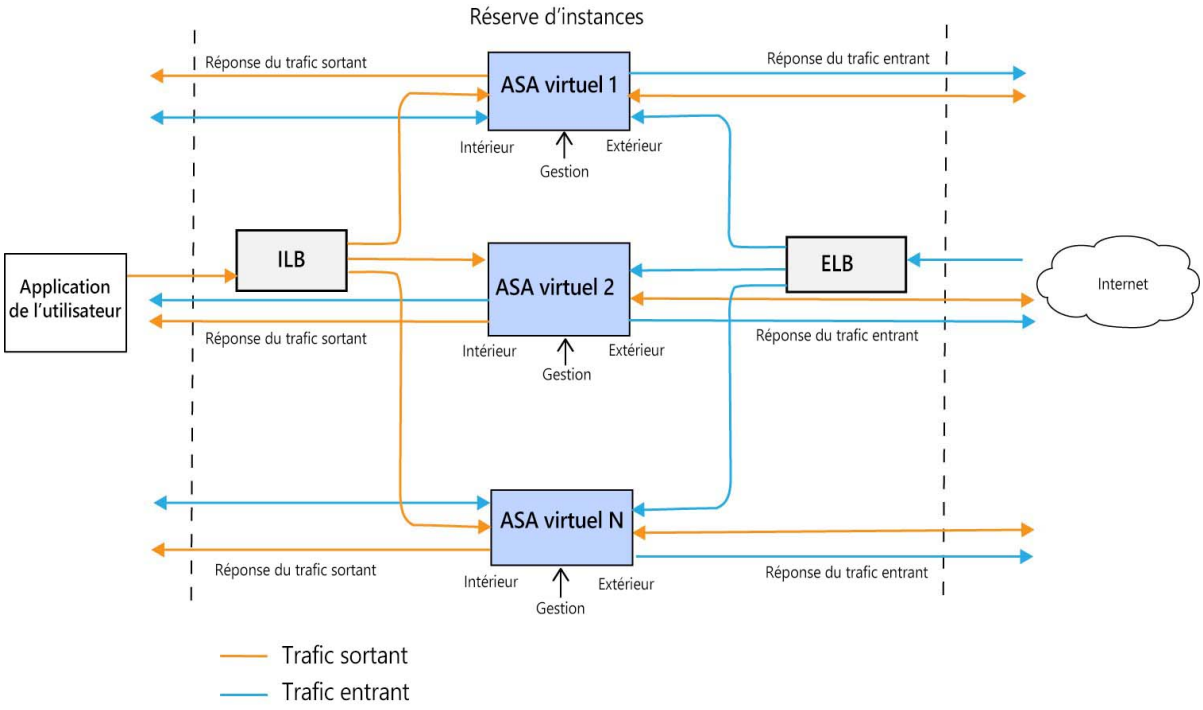
Déployer la solution d'évolutivité automatique ASA virtuel sur OCI

- Scénario , à la page 231
- Prérequis, à la page 232
- Préparation du fichier de configuration ASA, à la page 238
- Déployer la solution d'évolutivité automatique, à la page 244
- Valider le déploiement, à la page 249
- Mise à niveau, à la page 250
- Supprimer la configuration d'évolutivité automatique d'OCI, à la page 251

Scénario

Le scénario pour cet ASA virtuel : la solution d'évolutivité automatique OCI est illustrée dans le diagramme des scénarios. L'équilibreur de charges Internet a une adresse IP publique et des ports activés à l'aide d'une combinaison de l'écouteur et du groupe cible.

Illustration 52 : Diagramme de scénario



Le partage basé sur le port peut être mi en œuvre pour le trafic réseau. Cela peut être réalisé en utilisant des règles NAT. Cet exemple de configuration est expliqué dans les sections suivantes.

Prérequis

Autorisations et politiques

Voici les autorisations et les politiques OCI dont vous avez besoin pour implémenter la solution :

1. **Utilisateurs et groupe**

Remarque Vous devez être un utilisateur OCI ou un administrateur de location pour créer les utilisateurs et les groupes.

Créez des comptes d'utilisateurs Oracle Cloud Infrastructure et un groupe auquel ces comptes d'utilisateurs appartiennent. Si le groupe approprié avec les comptes d'utilisateurs existe, vous n'avez pas besoin de les créer. Pour obtenir des instructions sur la création des utilisateurs et des groupes, consultez Création de groupes et d'utilisateurs.

2. **Politiques de groupe**

   Vous devez créer les politiques, puis les mapper au groupe. Pour créer les politiques, accédez à **OCI** > **Identity & Security (Identité et sécurité)** > **Policies (Politiques)** > **Create Policy (Créer une politique)**. Créez et ajoutez les politiques suivantes au groupe souhaité :

- Autoriser le groupe <*Group_Name*> à utiliser les mesures dans le compartiment <*Compartment_Name*>
- Autoriser le groupe <*Group_Name*> à gérer les alarmes dans le compartiment <*Compartment_Name*>
- Autoriser le groupe <*Group_Name*> à gérer les sujets pertinents dans le compartiment <*Compartment_Name*>
- Autoriser le groupe <*Group_Name*> à inspecter les mesures dans le compartiment <*Compartment_Name*>
- Autoriser le groupe <*Group_Name*> à lire les mesures dans le compartiment <*Compartment_Name*>
- Autoriser le groupe <*Group_Name*> à utiliser des espaces de noms de balises dans le compartiment <*Compartment_Name*>
- Autoriser le groupe <*Group_Name*> à lire les groupes de journaux dans le compartiment <*Compartment_Name*>
- Autoriser le groupe <*Group_Name*> à utiliser le compartiment de regroupement d'instances <*Compartment_Name*>
- Autoriser le groupe <*Group_Name*> à utiliser Cloud Shell dans la location
- Autoriser le groupe <*Group_Name*> à lire l'espace de nom du stockage d'objets dans la location
- Autoriser le groupe <*Group_Name*> à gérer les référentiels dans la location

Remarque Vous pouvez également créer des politiques au niveau de la location. Vous êtes libre de décider comment vous souhaitez accorder toutes les autorisations.

3. **Autorisation pour les fonctions Oracle**

   Pour permettre à une fonction Oracle d'accéder à une autre ressource d'Oracle Cloud Infrastructure, incluez la fonction dans un groupe dynamique, puis créez une politique pour accorder l'accès du groupe dynamique à cette ressource.

4. **Créer un groupe dynamique**

   Pour créer des groupes dynamiques, accédez à **OCI** > **Identity & Security (Identité et sécurité)** > **Dynamic Group (Groupe dynamique)** > **Create Dynamic Group (Créer un groupe dynamique)**

   Précisez la règle suivante lors de la création du groupe dynamique :

   ```
   TOUS {resource.type = « fnfunc », resource.compartment.id = « <Your_Compartment_OCID> »}
   ```

   Pour en savoir plus sur les groupes dynamiques, consultez :

   - https://docs.oracle.com/en-us/iaas/Content/Functions/Tasks/functionsaccessingociresources.htm
   - https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm

5. **Créer une politique pour un groupe dynamique**

   Pour ajouter une politique, accédez à **OCI** > **Identity & Security (Identité et sécurité)** > **Policies (Politiques)** > **Create Policy (Créer une politique)**. Ajoutez la politique suivante au groupe :

```
Autoriser le groupe dynamique <Dynamic_Group_Name> à gérer toutes les ressources dans
le compartiment <Compartment_OCID>
```

Téléchargez les fichiers à partir de GitHub

ASA virtuel : la solution d'évolutivité automatique OCI est fournie en tant que référentiel GitHub. Vous pouvez extraire ou télécharger les fichiers du référentiel.

Environnement Python 3

Un fichier *make.py* se trouve dans le référentiel cloné. Ce programme compresse les fonctions oracle et les fichiers de modèle dans un fichier Zip; copiez-les dans un dossier cible. Afin d'effectuer ces tâches, l'environnement Python 3 doit être configuré.

Remarque Ce script Python ne peut être utilisé que dans l'environnement Linux.

Configuration de l'infrastructure

Les éléments suivants doivent être configurés :

1. **VCN**

   Créez le VCN selon les besoins de votre application ASA virtuel. Créez le VCN avec la passerelle Internet ayant au moins un sous-réseau associé à une route vers Internet.

   Pour en savoir plus sur la création du VCN, consultez https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/creatingnetwork.htm.

2. **Sous-réseaux d'application**

   Créez des sous-réseaux selon les besoins de votre application ASA virtuel. Pour implémenter la solution selon ce scénario, l'instance ASA virtuel nécessite trois sous-réseaux pour fonctionner.

   Pour en savoir plus sur la création d'un sous-réseau, consultez https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingVCNs_topic-Overview_of_VCNs_and_Subnets.htm#.

3. **Sous-réseau externe**

   Le sous-réseau doit avoir une route avec « 0.0.0.0/0 » vers la passerelle Internet. Ce sous-réseau contient l'interface externe de Cisco ASA virtuel et l'équilibreur de charges sur Internet. Assurez-vous que la passerelle NAT est ajoutée pour le trafic sortant.

   Pour en savoir plus, consultez les documents suivants :

   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIGs.htm
   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/NATgateway.htm#To_create_a_NAT_gateway

4. **Sous-réseau interne**

   Ceci est similaire aux sous-réseaux d'application, avec ou sans passerelle NAT/Internet.

Remarque Pour les sondes d'intégrité ASA virtuel, vous pouvez atteindre le serveur de métadonnées (169.254.169.254) par le port 80.

5. **Management Subnet** (Sous-réseau de gestion)

   Le sous-réseau de gestion doit être public afin de prendre en charge l'accessibilité SSH avec ASA virtuel.

6. **Groupes de sécurité – Groupe de sécurité réseau pour l'instance ASA virtuel**

   Configurez le groupe de sécurité pour les instances ASA virtuel qui répondent aux exigences suivantes :

   - Les fonctions Oracle (dans le même VCN) établissent des connexions SSH à l'adresse de gestion de ASA virtuel.
   - Les hôtes d'administration peuvent avoir besoin d'un accès SSH aux instances d'ASA virtuel.
   - L'ASA virtuel initie la communication avec les serveurs CSSM/satellite pour les licences.

7. **Espace de nom du stockage d'objets**

   Cet espace de nom du stockage d'objets est utilisé pour l'hébergement d'un site Web statique, ayant le fichier configuration.txt. Vous devez créer des demandes préauthentifiées pour le fichier configuration.txt. Cette URL préauthentifiée est utilisée lors du déploiement du modèle.

Remarque Assurez-vous que les configurations suivantes qui sont chargées sont accessibles par les instances de ASA virtuel par l'intermédiaire de l'URL HTTP.

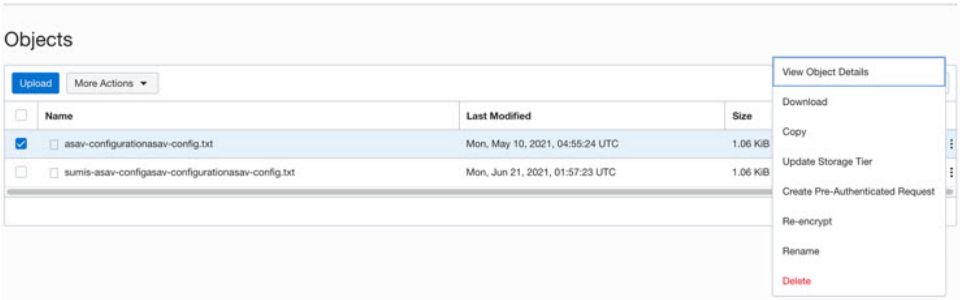
Lorsque ASA virtuel est démarré, il exécute la commande suivante`$ copy /noconfirm <URL de demande préauthentifiée du fichier configuration.txt > disk0:Configuration.txt`

Cette commande permet de configurer le lancement de ASA virtuel avec le fichier configuration.txt.

8. **Charger le fichier configuration.txt**

   Pour créer une URL de demande préauthentifiée du fichier de configuration ASA virtuel :

   1. Cliquez sur **Buckets (Compartiments)** > **Create Bucket (Créer un compartiment)**.
   2. Cliquez sur **Upload** (Charger).
   3. Lorsque le fichier de configuration est chargé, choisissez **Create Pre-Authenticated Request** (Créer une demande préauthentifiée) comme illustré dans la figure ci-dessous.



Remarque Le fichier de configuration devrait maintenant être accessible à partir de la fonction oracle.

Configuration du réseau

1. **Trafic entrant**

   Assurez-vous que l'adresse *<IP de la VM d'application>* est correcte dans configuration.txt, comme mentionné dans Configuration des objets, des licences, des règles NAT et des politiques d'accès.

2. **Trafic sortant**

   - Assurez-vous que l'adresse *<IP du serveur externe>* est correcte dans configuration.txt, comme mentionné dans Configuration des objets, des licences, des règles NAT et des politiques d'accès.
   - Assurez-vous qu'il y a une passerelle NAT dans votre VCN externe.
   - Assurez-vous d'ajouter la même adresse *<IP du serveur externe>* dans la table de routage de votre VCN externe, à destination de la passerelle NAT, comme illustré dans l'exemple ci-dessous :

Destination	Target Type	Target
0.0.0.0/0	Internet Gateway	outside-ig
8.8.8.8/32	NAT Gateway	nat-gw

Chiffrer le mot de passe

Remarque Pour en savoir plus sur cette procédure, consultez Créer des vaults et des secrets.

Le mot de passe pour ASA virtuel est utilisé pour configurer toutes les instances de ASA virtuel utilisées lors de l'évolutivité automatique et il est utilisé pour récupérer les données d'utilisation du processeur (CPU) des instances ASA virtuel.

Par conséquent, vous devez enregistrer le mot de passe et le réinitialiser de temps en temps. En raison des modifications courantes et de la vulnérabilité, la modification ou l'enregistrement du mot de passe en texte brut n'est pas autorisée. Le mot de passe doit être en format chiffré uniquement.

Pour obtenir le mot de passe chiffré :

Procédure

Étape 1 Créez un vault.

OCI Vault fournit des services pour créer et enregistrer des clés de chiffrement principales en toute sécurité, et des méthodes de chiffrement et de déchiffrement pour leur utilisation. Vault doit donc être créé (si ce n'est déjà fait) dans le même compartiment que le reste de la solution d'évolutivité automatique.

Accédez à **OCI** > **Identity & Security (identitié et sécurité)** > **Vault** > **Choose or Create a new Vault (choisir ou créer un nouveau vault)**

.

Étape 2 Créez une clé de chiffrement principale.

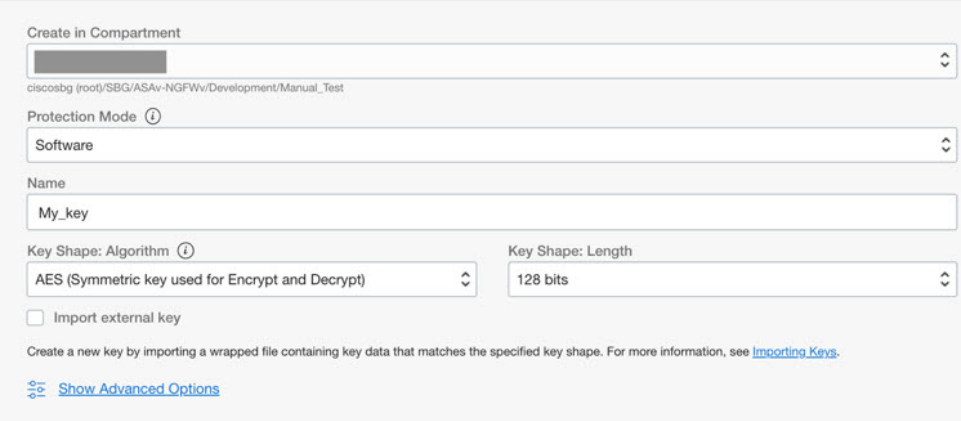
Une clé de chiffrement principale est nécessaire pour chiffrer le mot de passe en texte brut.

Accédez à **OCI** > **Identity & Security (identitié et sécurité)** > **Vault** > **Choose or Create Key (choisir ou créer une clé)**

Choisissez l'une des clés de l'algorithme donné avec n'importe quel bit de longueur.

1. AES – 128, 192, 256
2. RSA – 2048, 3072, 4096
3. ECDSA – 256, 384, 521

Illustration 53 : Créer une clé



Étape 3 Créez un mot de passe chiffré.

1. Accédez à **OCI** > **Open CloudShell (OCI Cloud Terminal)** (ouvrir CloudShell (terminal OCI Cloud)).
2. Exécutez la commande suivante en remplaçant <*Password*> par votre mot de passe.

   ```
   echo -n '<Password>' | base64
   ```
3. À partir du Vault sélectionné, copiez le terminal cryptographique et l'OCID de la clé de chiffrement principale. Remplacez les valeurs suivantes, puis exécutez la commande de chiffrement :
   - KEY_OCID avec l'OCID de votre clé
   - Cryptographic_Endpoint_URL avec l'URL du terminal cryptographique de votre Vault
   - Password avec votre mot de passe

   Commande de chiffrement

   ```
   oci kms crypto encrypt --key-id Key_OCID --endpoint

   Cryptographic_Endpoint_URL --plaintext <base64-value-of-password>
   ```

4. Copiez le texte chiffré à partir de la sortie de la commande ci-dessus et utilisez-le selon vos besoins.

Préparation du fichier de configuration ASA

Assurez-vous que l'application est déployée ou que son plan de déploiement est disponible.

Procédure

Étape 1 Collectez les paramètres d'entrée suivants avant le déploiement :

Paramètre	Type de données	Description
tenancy_ocid	Chaîne	OCID de la location à laquelle votre compte appartient. Pour savoir comment trouver votre OCID de location, consultez ici. L'OCID de location ressemble à ceci : `ocid1.tenancy.oc1..`<ID_unique>
compartment_id	Chaîne	L'OCID du compartiment dans lequel créer les ressources. Exemple : `locid1.compartment.oc1..`<ID_unique>
compartment_name	Chaîne	Nom du compartiment
région	Chaîne	Identificateur unique de la région dans laquelle vous souhaitez que les ressources soient créées. Exemple : `us-phoenix-1, us-ashburn-1`
lb_size	Chaîne	Un modèle qui détermine la bande passante préprovisionnée totale (entrée plus sortie) de l'équilibreur de charges externe et interne. Valeurs prises en charge : 100 Mbit/s, 10 Mbit/s, 10 Mbit/s-Micro, 400 Mbit/s, 8 000 Mbit/s Exemple : 100 Mbit/s

Paramètre	Type de données	Description
availability_domain	Valeurs séparées par des virgules	Exemple : Tpeb:PHX-AD-1 **Remarque** Exécutez la commande **oci iam availability-domain list** dans Cloud Shell pour obtenir les noms de domaine de disponibilité.
min_and_max_instance_count	Valeurs séparées par des virgules	Le nombre minimal et maximal d'instances que vous souhaitez conserver dans le groupe d'instances. Exemple : 1,5
autoscale_group_prefix	Chaîne	Le préfixe à utiliser pour nommer toutes les ressources créées à l'aide du modèle. Par exemple, si le préfixe de ressource est « autoscale », toutes les ressources sont nommées comme suit : autoscale_resource1, autoscale_resource2, etc.
asav_config_file_url	URL	L'URL du fichier de configuration chargé dans le stockage d'objets à utiliser pour configurer l'ASA virtuel. **Remarque** L'URL de demande préauthentification du fichier de configuration doit être donnée. Exemple : https://objectstorage.<nom-region>.oraclecloud.com/<nom-objet-stockage>/oci-asav-configuration.txt
mgmt_subnet_ocid	Chaîne	OCID du sous-réseau de gestion qui doit être utilisé.
inside_subnet_OCID	Chaîne	OCID du sous-réseau interne qui doit être utilisé.
outside_subnet_ocid	Chaîne	OCID du sous-réseau externe qui doit être utilisé.
mgmt_nsg_ocid	Chaîne	OCID du groupe de sécurité réseau du sous-réseau de gestion qui doit être utilisé.
inside_nsg_ocid	Chaîne	OCID du groupe de sécurité réseau du sous-réseau interne qui doit être utilisé.

Paramètre	Type de données	Description
outside_nsg_ocid	Chaîne	OCID du groupe de sécurité réseau du sous-réseau externe qui doit être utilisé.
elb_listener_port	Valeurs séparées par des virgules	Liste des ports de communication pour l'écouteur de l'équilibreur de charges externe. Exemple : 80
ilb_listener_port	Valeurs séparées par des virgules	Liste des ports de communication pour l'écouteur de l'équilibreur de charges interne. Exemple : 80
health_check_port	Chaîne	Le port du serveur principal de l'équilibreur de charges par rapport auquel la vérification d'intégrité est exécutée. Exemple : 8080
instance_shape	Chaîne	La forme de l'instance à créer. La forme détermine le nombre de CPU, la quantité de mémoire et d'autres ressources qui sont allouées à l'instance. Formes prises en charge : « VM.Standard2.4 » et « VM.Standard2.8 »
lb_bs_policy	Chaîne	La politique d'équilibreur de charges à utiliser pour l'ensemble principal de l'équilibreur de charges interne et externe. Pour en savoir plus sur le fonctionnement des politiques d'équilibreur de charges, consultez ce lien. Valeurs prises en charge : « ROUND_ROBIN », « LEAST_CONNECTIONS », « IP_HASH »

Paramètre	Type de données	Description
image_name	Chaîne	Le nom de l'image de Marché à utiliser pour créer la configuration d'instance. Valeur par défaut : « Cisco ASA virtual firewall (ASAv) » (pare-feu virtuel Cisco ASA (ASAv)) **Remarque** Si l'utilisateur souhaite déployer une image personnalisée, il doit configurer le paramètre custom_image_ocid.
image_version	Chaîne	La version de l'image ASA virtuel disponible dans le Marché OCI à utiliser. Actuellement, les versions 9.15.1.15 et 9.16.1 sont disponibles. Valeur par défaut : « Cisco ASA virtual firewall (ASAv) » (pare-feu virtuel Cisco ASA (ASAv))
scaling_thresholds	Valeurs séparées par des virgules	Les seuils d'utilisation du CPU à utiliser pour l'évolutivité à la baisse ou à la hausse. Précisez les valeurs de seuil d'évolutivité à la baisse et à la hausse séparées par des virgules. Exemple : 15,50 où 15 est le seuil d'évolutivité à la baisse et 50 est le seuil d'évolutivité à la hausse.
custom_image_ocid	Chaîne	OCID de l'image personnalisée à utiliser pour créer la configuration de l'instance si l'image du Marché ne doit pas être utilisée. **Remarque** custom_image_ocid est un paramètre facultatif
asav_password	Chaîne	Le mot de passe pour ASA virtuel sous forme chiffrée, en utilisant le protocole SSH dans l'ASA virtuel pour la configuration. Utilisez le guide de configuration pour les instructions sur la façon de chiffrer le mot de passe ou consultez ce lien.

Paramètre	Type de données	Description
cryptographic_endpoint	Chaîne	Le terminal cryptographique est une URL utilisée pour déchiffrer le mot de passe. Il se trouve dans le Vault (centre de stockage).
master_encryption_key_id	Chaîne	L'OCID de la clé avec laquelle le mot de passe a été chiffré. Il se trouve dans le Vault (centre de stockage).
Profile Name (Nom de profil)		Il s'agit du nom de profil de l'utilisateur dans OCI. Il se trouve dans la section du profil de l'utilisateur. Exemple : oracleidentitycloudservice/<utilisateur>@<mail>.com
Object Storage Namespace (espaces de nom du stockage d'objet)		Il s'agit d'un identifiant unique créé au moment de la création de la location. Vous pouvez trouver cette valeur dans **OCI** > **Administration** > **Tenancy Details (détails de la location)**
Jeton d'autorisation		Il est utilisé comme mot de passe pour la connexion au docker, qui autorise l'envoi d'Oracle-Functions dans le registre de conteneur OCI. Pour se procurer le jeton, accédez à **OCI** > **Identity (identité)** > **Users (utilisateurs)** > **User Details (détails de l'utilisateur** > **) Auth Tokens (jetons d'autorisation)** > **Generate Token (générer un jeton)**.

Étape 2 Configurez les objets, les licences, la règle NAT pour les sondes d'intégrité de l'équilibreur de charges et les politiques d'accès.

```
! Default route via outside
route outside 0.0.0.0 0.0.0.0 <Outside Subnet gateway> 2

! Health Check Configuration
object network metadata-server
host 169.254.169.254
object service health-check-port
service tcp destination eq <health-check-port>
object service http-port
service tcp destination eq <traffic port>
route inside 169.254.169.254 255.255.255.255 <Inside Subnet GW> 1

! Health check NAT
nat (outside,inside) source static any interface destination static interface metadata-server service
 health-check-port http-port
nat (inside,outside) source static any interface destination static interface metadata-server service
 health-check-port http-port
```

```
! Outbound NAT
object network inside-subnet
subnet <Inside Subnet> <Inside Subnet Gateway>
object network external-server
host <External Server IP>
nat (inside,outside) source static inside-subnet interface destination static interface
external-server

! Inbound NAT
object network outside-subnet
subnet <Outside Subnet> <Outside Subnet GW>
object network http-server-80
host <Application VM IP>
nat (outside,inside) source static outside-subnet interface destination static interface
http-server-80

!
dns domain-lookup outside
DNS server-group DefaultDNS

! License Configuration
call-home
profile license
destination transport-method http
destination address http <URL>
debug menu license 25 production
license smart
feature tier standard
throughput level <Entitlement>
licence smart register idtoken <License token> force
!
```

Ces connexions de sonde d'intégrité et cette configuration de plan de données doivent être autorisées sur la politique d'accès.

Étape 3 Mettez à jour le fichier *configuration.txt* avec les détails de la configuration.

Étape 4 Chargez le fichier *configuration.txt* dans l'espace de stockage d'objets créé par l'utilisateur et créez la demande de préauthentification pour le fichier chargé.

Remarque
Assurez-vous que l'URL de demande de préauthentification du fichier configuration.txt est utilisée dans le déploiement de la pile.

Étape 5 Créez des fichiers zip.

Un fichier *make.py* se trouve dans le référentiel cloné. Exécutez la commande `python3 make.py build` pour créer les fichiers zip. Le dossier cible contient les fichiers suivants.

```
Tue Jun 08 07:46 AM [sumis@SUMIS-M-41KG target]$ tree -A
.
├── Oracle-Functions.zip
├── asav_autoscale_deploy.zip
├── asav_configuration.txt
├── deploy_oracle_functions_cloudshell.py
├── template1.zip
└── template2.zip

0 directories, 6 files
Tue Jun 08 07:46 AM [sumis@SUMIS-M-41KG target]$
```

Remarque
Si vous déployez la solution d'évolutivité automatique à l'aide de Cloud Shell, mettez à jour le fichier *easy_deploy/deployment_parameters.json* avant d'exécuter la commande `python3 make.py build`. Pour la mise à jour, reportez-vous à Collecte des paramètres d'entrée et Déploiement des fonctions Oracle.

Déployer la solution d'évolutivité automatique

Après avoir effectué les étapes préalables au déploiement, commencez à créer la pile OCI. Vous pouvez effectuer un déploiement manuel ou effectuer undéploiement à l'aide de Cloud Shell. Les scripts et les modèles de déploiement pour votre version sont disponibles dans le référentiel GitHub.

Déploiement manuel

Le déploiement de la solution d'évolutivité automatique de bout en bout comprend trois étapes : déployer la pile Terraform Template-1, déployer les fonctions Oracle, puis déployer Terraform Template-2.

Déployer la pile Terraform Template-1

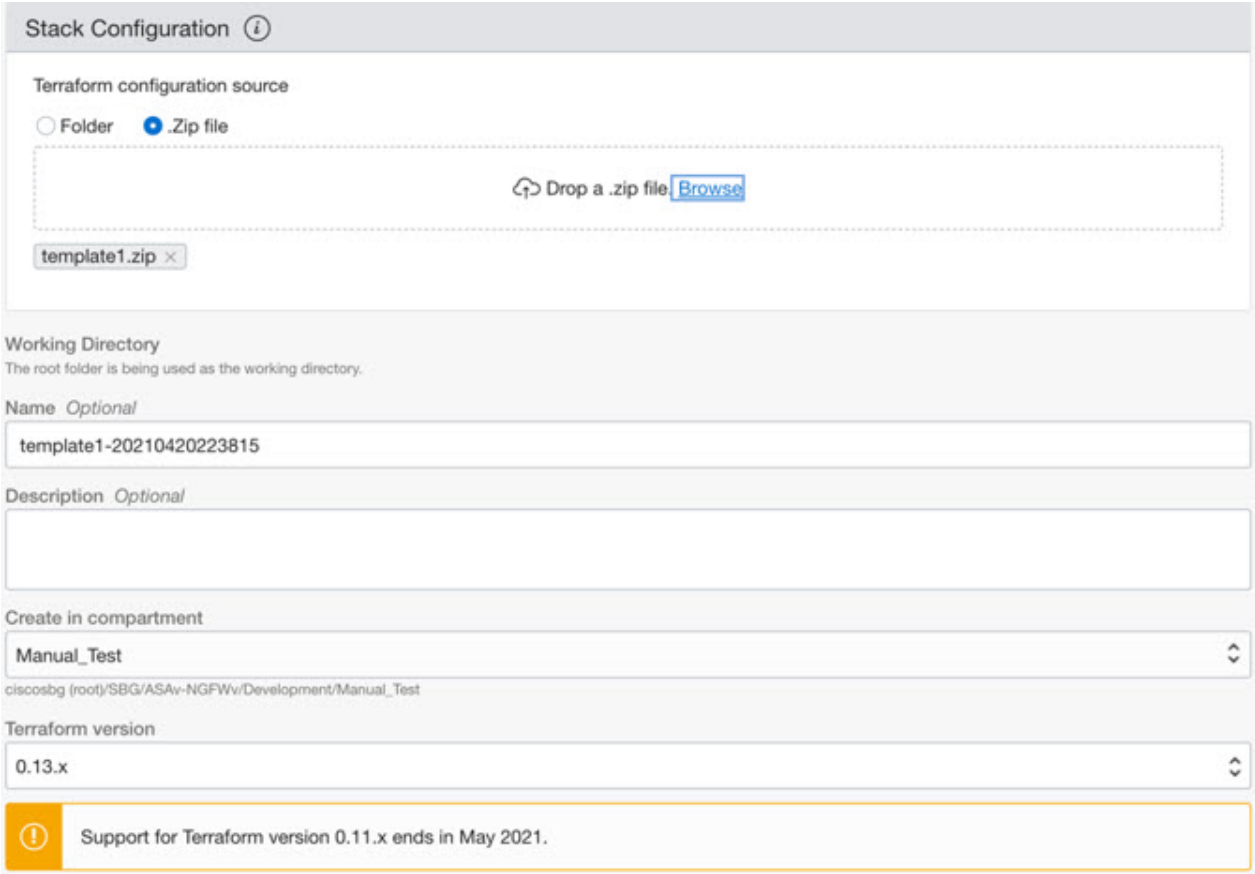
Procédure

Étape 1 Connectez-vous au portail OCI.

La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.

Étape 2 Choisissez **Developer Service (Service de développeur)** > **Resource Manager (Gestionnaire de ressources)** > **Stack (Pile)** > **Create Stack (Créer une pile)**.

Choisissez **My Configuration** (Ma configuration), puis sélectionnez le fichier *Terraform template1.zip* dans le dossier cible en tant que source de configuration Terraform, comme illustré dans la figure ci-dessous.



Étape 3 Dans la liste déroulante **Transform version** (Version de Transform), sélectionnez 0.13.x ou 0.14.x.

Étape 4 À l'étape suivante, saisissez tous les détails recueillis dans Collecte des paramètres d'entrée.

Remarque
Saisissez des paramètres d'entrée valides, sans quoi le déploiement de la pile pourrait échouer à d'autres étapes.

Étape 5 À l'étape suivante, choisissez **Terraform Actions (Actions Terraform)** > **Apply (Appliquer)**.

Une fois le déploiement réussi, procédez au déploiement des fonctions Oracle.

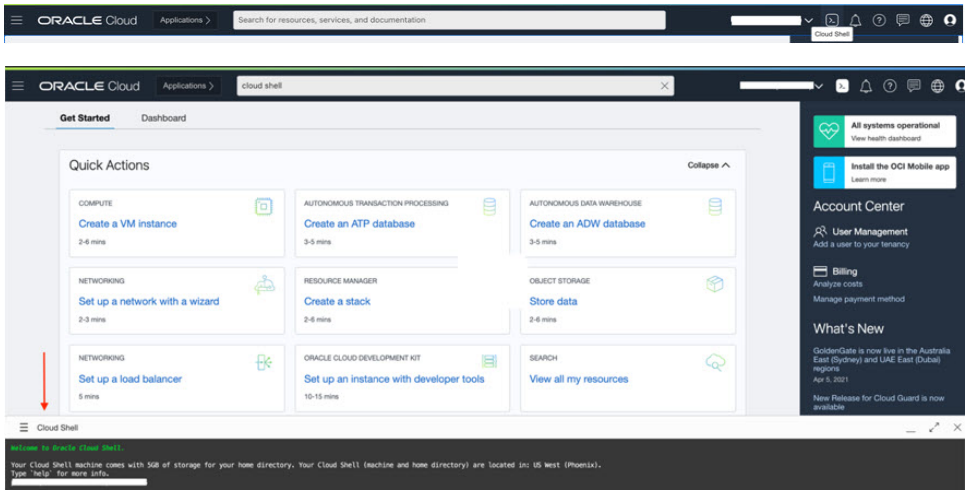
Déployer les fonctions Oracle

Remarque *Cette étape doit être effectuée uniquement après le déploiement réussi de Terraform Template-1.*

Dans OCI, les fonctions Oracle sont chargées en tant qu'images Docker, qui sont enregistrées dans le registre de conteneur OCI. Les fonctions Oracle doivent être poussées dans l'une des applications OCI (créées dans Terraform Template-1) au moment du déploiement.

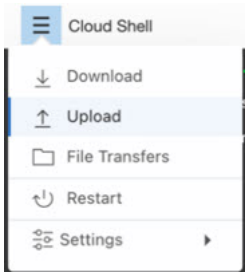
Procédure

Étape 1 Ouvrez OCI Cloud Shell.

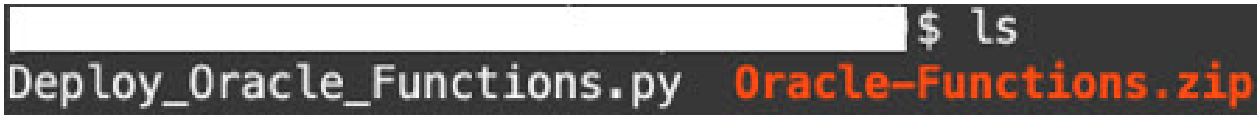


Étape 2 Chargez *deploy_oracle_functions_cloudshell.py* et *Oracle-Functions.zip*.

Dans le menu contextuel de Cloud Shell, choisissez **Upload** (Charger).



Étape 3 Vérifiez les fichiers à l'aide de la commande **ls**.



Étape 4 Exécutez `python3 Deploy_Oracle_Functions.py -h`. Le script `deploy_oracle_functions_cloudshell.py` nécessite certains paramètres d'entrée dont les détails peuvent être trouvés à l'aide de l'argument d'aide, comme illustré dans la figure ci-dessous.

```
                                $ python3 Deploy_Oracle_Functions.py -h
usage: Deploy_Oracle_Functions.py [-h] -a  -r  -p  -c  -o  -t

*** Script to deploy Oracle Function for OCI ASAv Autoscale Solution ***

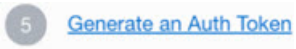
Instruction to find values of required arguments:
Application Name: Name of Application created by first Terraform Template
Region Identifier: OCI -> Administration -> Region Management
Profile Name: OCI -> Profile
Compartment OCID: OCI -> Identity -> Compartment -> Compartment Details
Object Storage Namespace: OCI -> Administration -> Tenancy Details
Authorization Token: OCI -> Identity -> Users -> User Details -> Auth Tokens -> Generate Token

optional arguments:
  -h, --help  show this help message and exit
  -a          Name of Application in OCI to which functions will be deployed
  -r          Region Identifier
  -p          Profile Name of User
  -c          Compartment OCID
  -o          Object Storage Namespace
  -t          Authorization Token for Docker Login (*Please Put in Quotes)
```

Pour exécuter le script, transmettez les arguments suivants :

Tableau 24 : Arguments et détails

Argument	Détails
Nom de l'application	Il s'agit du nom de l'application OCI créée par le déploiement de Terraform Template-1. Sa valeur est obtenue en combinant **« autoscale_group_prefix »** dans le Template-1 et le suffixe **« _application ».**
Identifiant de région	L'identifiant de région est le mot de code de région fixé dans OCI pour différentes régions. Par exemple : « us-phoenix-1 » pour Phoenix ou « ap-melbourne-1 » pour Melbourne. Pour obtenir la liste de toutes les régions avec leurs identifiants de région, accédez à **OCI** > **Administration** > **Region Management (Gestion de la région)**.
Nom de profil	Il s'agit du nom de profil de l'utilisateur simple dans OCI. Exemple : *oracleidentitycloudservice/<user>@<mail>.com* Le nom se trouve dans la section du profil de l'utilisateur.
OCID du compartiment	Il s'agit de l'OCID (Oracle Cloud Identifier) du compartiment. OCID du compartiment où l'utilisateur dispose de l'application OCI. Accédez à **OCI** > **Identity (Identité)** > **Compartment (Compartiment)** > **Compartment Details (Détails du compartiment)**.
Espace de nom du stockage d'objets	Il s'agit d'un identifiant unique créé au moment de la création de la location. Accédez à **OCI** > **Administration** > **Tenancy Details (Détails de la location)**.

Argument	Détails
Jeton d'autorisation	Il est utilisé comme mot de passe pour la connexion au docker, ce qui l'autorise à pousser les fonctions Oracle dans le registre de conteneur OCI. Précisez le jeton entre guillemets dans le script de déploiement. Accédez à **OCI** > **Identity (Identité)** > **Users (Utilisateurs)** > **User Details (Détails de l'utilisateur)** > **Auth Tokens (Jetons d'autorisation)** > **Generate Token (Générer un jeton)**. Si, pour quelque raison que ce soit, vous ne parvenez pas à afficher les détails de l'utilisateur, cliquez sur **Developer services (Services de développeur)** > **Functions (Fonctions)**. Accédez à l'application créée par Terraform Template-1. Cliquez sur **Getting Started** (Mise en route) et choisissez Cloud Shell Setup (Configuration de Cloud Shell). Parmi les étapes, vous trouverez le lien pour générer un jeton d'authentification, comme illustré ci-dessous. 

Étape 5 Exécutez la commande `python3 Deploy_Oracle_Functions.py` en transmettant des arguments d'entrée valides. Le déploiement de toutes les fonctions prendra un certain temps. Vous pouvez ensuite supprimer le fichier et fermer Cloud Shell.

Déployer Terraform Template-2

Template 2 déploie les ressources liées à la création d'alarmes, y compris les alarmes et les sujets ONS pour la fonction d'appel. Le déploiement de Template 2 est similaire au déploiement deTerraform Template-1.

Procédure

Étape 1 Connectez-vous au portail OCI.

La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.

Étape 2 Choisissez **Developer Service (service de développeur)** > **Resource Manager (gestionnaire de ressources)** > **Stack (pile)** > **Create Stack (créer une pile)**.

Sélectionnez *Terraform template template2.zip* dans le dossier cible comme source de la configuration de Terraform.

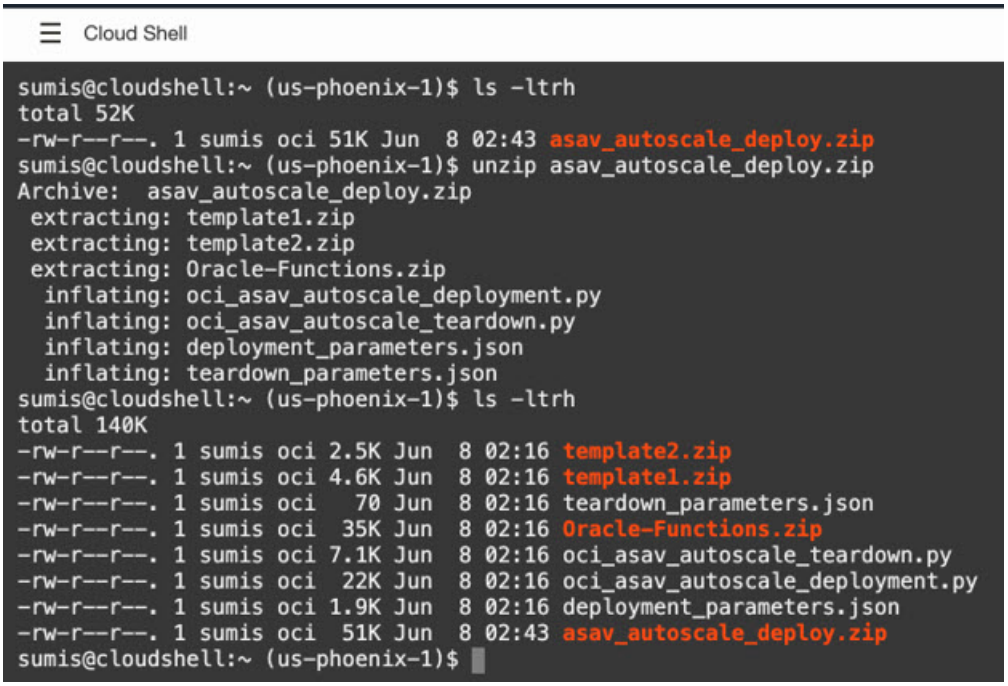
Étape 3 À l'étape suivante, cliquez sur **Terraform Actions (actions Terraform)** > **Apply (appliquer)**.

Déployer l'évolutivité automatique à l'aide de Cloud Shell

Pour éviter les frais généraux de déploiement, vous pouvez invoquer le script de déploiement de bout en bout facile pour déployer la solution d'évolutivité automatique (fonctions Terraform template1, template2 et oracle).

Procédure

Étape 1 Chargez le fichier *asav_autoscale_deploy.zip* dans le dossier cible de l'interface Cloud Shell et extrayez les fichiers.



Étape 2 Assurez-vous d'avoir mis à jour les paramètres d'entrée dans le *deployment_parameters.json* avant d'exécuter la commande `python3 make.py`.

Étape 3 Pour commencer à déployer la solution d'évolutivité automatique, exécutez la commande `python3 oci_asav_autoscale_deployment.py` sur l'interface Cloud Shell.

Le déploiement de la solution prendra environ 10 à 15 minutes.

Si une erreur survient pendant le déploiement de la solution, le journal des erreurs est enregistré.

Valider le déploiement

Validez si toutes les ressources sont déployées et que les fonctions Oracle sont connectées avec des alarmes et des événements. Par défaut, le regroupement d'instances a un nombre minimal et maximal d'instances à zéro. Vous pouvez modifier le regroupement d'instances dans l'interface utilisateur d'OCI avec le nombre minimal et maximal que vous souhaitez. Cela déclenchera de nouvelles instances ASA virtuel.

Nous vous recommandons de lancer une seule instance, de vérifier son flux de travail et de valider son comportement pour vous assurer qu'elle fonctionne comme prévu. Après cette validation, vous pouvez déployer les exigences réelles de ASA virtuel.

Remarque Précisez le nombre minimal d'instances ASA virtuel comme **protégé contre une évolutivité à la baisse** pour éviter qu'elles soient supprimées par les politiques d'évolutivité d'OCI.

Mise à niveau

Mettre à niveau la pile d'évolutivité automatique

Aucune prise en charge de la mise à niveau dans cette version. Les piles doivent être redéployées.

Mettre à niveau les machines virtuelles ASA virtuel

Aucune prise en charge de la mise à niveau des machines virtuelles ASA virtuel dans cette version. La pile doit être redéployée avec l'image ASA virtuel requise.

Réserve d'instances

1. Pour modifier le nombre minimum et maximum d'instances dans le groupe d'instances :

   Cliquez sur **Developer Services (Services de développeurs)** > **Function (Fonction)** > **Application Name (Nom de l'application) (créé par Terraform Template 1)** > **Configuration**.

   Modifiez respectivement min_instance_count et max_instance_count.

2. La suppression/résiliation de l'instance n'est pas l'équivalent d'une évolutivité à la baisse. Si une instance de la réserve d'instances est supprimée/résiliée en raison d'une action externe et non d'une action d'évolutivité à la baisse, la réserve d'instances lance automatiquement une nouvelle instance à récupérer.

3. Max_instance _count définit la limite de seuil pour l'action d'évolutivité à la hausse, mais elle peut être dépassée en modifiant le nombre d'instances de la réserve d'instances à l'aide de l'interface utilisateur. Assurez-vous que le nombre d'instances de l'interface utilisateur est inférieur au max_instance_count défini dans l'application OCI. Sinon, augmentez le seuil en conséquence.

4. La réduction du nombre d'instances dans la réserve d'instances directement à partir de l'application n'effectue pas les actions de nettoyage définies par programmation. En raison de quoi les systèmes dorsaux ne seront pas purgés et supprimés des deux équilibreurs de charges, si ASA virtuel a une licence, elle sera perdue.

5. Pour certaines raisons, si l'instance ASA virtuel n'est pas intègre, ne répond pas et est inaccessible par SSH pendant une période définie, l'instance est supprimée de la réserve d'instances avec force, et des licences peuvent être perdues.

Fonctions Oracle

- Les fonctions Oracle sont en fait des images de Docker. Ces images sont enregistrées dans le répertoire racine du registre de conteneur OCI. Ces images ne doivent pas être supprimées, car cela supprimera également la fonction utilisée dans la solution d'évolutivité automatique.
- L'application OCI créée par Terraform template-1 contient des variables environnementales essentielles, qui sont requises par les fonctions Oracle pour fonctionner correctement. Ni la valeur ni le format de ces

variables d'environnement ne doivent être modifiés, sauf si cela est obligatoire. Toutes les modifications apportées sont reflétées dans les nouvelles instances uniquement.

Ensembles de systèmes principaux de l'équilibreur de charge

Dans OCI, la connexion de l'équilibreur de charges au groupe d'instances n'est prise en charge que par l'utilisation de l'interface principale configurée comme interface de gestion dans ASA virtuel. Par conséquent, l'interface interne est connectée à l'ensemble principal de l'équilibreur de charges interne; l'interface externe est connectée à l'ensemble principal de l'équilibreur de charges externe. Ces adresses IP ne sont pas automatiquement ajoutées ou supprimées de l'ensemble principal. La solution d'évolutivité automatique gère ces deux tâches de manière programmatique. Mais dans le cas d'une action, d'une maintenance ou d'un dépannage externe, il pourrait y avoir une situation nécessitant un effort manuel pour les utiliser.

Selon les besoins, d'autres ports peuvent être ouverts sur l'équilibreur de charges à l'aide d'un écouteur et d'ensembles principaux. Les adresses IP des instances à venir sont automatiquement ajoutées à l'ensemble principal, mais les adresses IP des instances existantes doivent être ajoutées manuellement.

Ajout d'un écouteur dans l'équilibreur de charges

Pour ajouter un port en tant qu'écouteur dans l'équilibreur de charges, accédez à **OCI** > **Networking (réseautage)** > **Load Balancer (équilibreur de charges)** > **Listener (écouteur)** > **Create Listener (créer un écouteur)**.

Enregistrer un système principal dans l'ensemble principal

Afin d'enregistrer une instance ASA virtuel sur l'équilibreur de charges, l'adresse IP de l'interface externe de l'instance ASA virtuel doit être configurée en tant que système principal dans l'ensemble principal de l'équilibreur de charges externe. L'adresse IP de l'interface interne doit être configurée comme système principal dans l'ensemble principal de l'équilibreur de charges interne. Assurez-vous que le port que vous utilisez a été ajouté dans l'écouteur.

Supprimer la configuration d'évolutivité automatique d'OCI

Les piles déployées à l'aide de Terraform peuvent être supprimées de la même manière, à l'aide du gestionnaire de ressources dans OCI. La suppression de la pile supprime toutes les ressources créées par celle-ci et tous les renseignements associés à ces ressources sont supprimés définitivement.

Remarque En cas de suppression de pile, il est recommandé de faire en sorte que le nombre minimal d'instances dans le groupe d'instances soit de 0 et d'attendre la fin des instances. Cela facilitera la suppression de toutes les instances et ne laissera aucune trace.

Vous pouvez effectuer une suppression manuelle ou utiliser Cloud Shell.

Suppression manuelle

La suppression de la solution d'évolutivité automatique de bout en bout se déroule en trois étapes : supprimer la pile Terraform Template-2, supprimer les fonctions Oracle, puis supprimer la pile Terraform Template-1.

Supprimer la pile Terraform Template-2

Pour supprimer la configuration de l'évolutivité automatique, vous devez commencer par supprimer la pile Terraform Template-2.

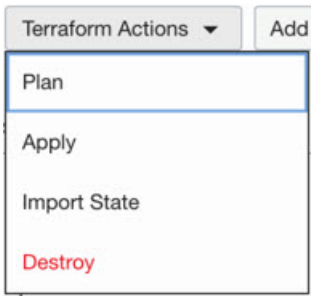
Procédure

Étape 1 Connectez-vous au portail OCI.

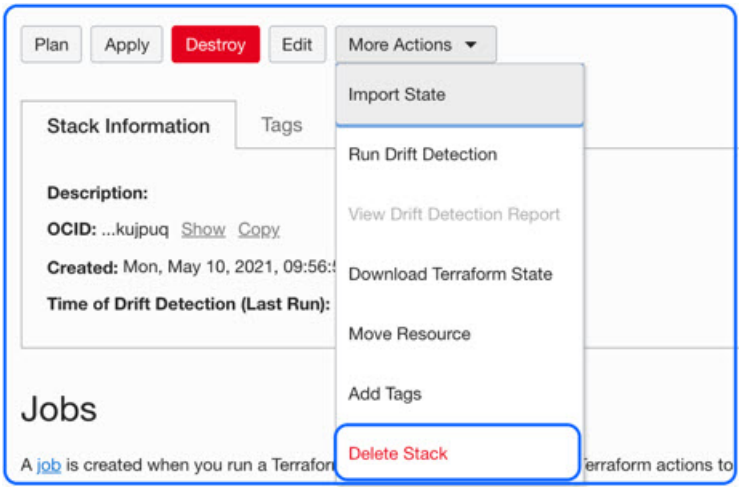
La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.

Étape 2 Choisissez **Developer Services (Services de développeur)** > **Resource Manager (Gestionnaire de ressources)** > **Stack (Pile)**.

Étape 3 Sélectionnez la pile créée par Terraform Template-2, puis sélectionnez **Destroy** (Détruire) dans le menu déroulant **Terraform Actions** (Actions Terraform) comme illustré dans la figure ci-dessous :



La tâche de destruction est créée, ce qui prend un certain temps pour supprimer des ressources les unes après les autres. Vous pouvez supprimer la pile une fois la tâche de destruction terminée, comme illustré dans la figure ci-dessous :



Étape 4 Procédez à la suppression des fonctions Oracle.

Supprimer les fonctions Oracle

Le déploiement des fonctions Oracle ne fait pas partie du déploiement de la pile Terraform Template, il est chargé séparément à l'aide de Cloud Shell. Par conséquent, sa suppression n'est pas non plus prise en charge par la suppression de la pile Terraform. Vous devez supprimer toutes les fonctions Oracle dans l'application OCI créée par Terraform Template-1.

Procédure

Étape 1 Connectez-vous au portail OCI.

La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.

Étape 2 Choisissez **Developer Services (Services de développeur)** > **Functions (Fonctions)**. Choisissez le nom de l'application qui a été créée dans la pile Template-1.

Étape 3 Dans cette application, visitez chaque fonction et supprimez-le.

Supprimer la pile Terraform Template-1

Remarque La suppression de la pile Template-1 de la pile ne réussira qu'après avoir supprimé toutes les fonctions Oracle.

Identique à la suppression de Terraform Template-2.

Procédure

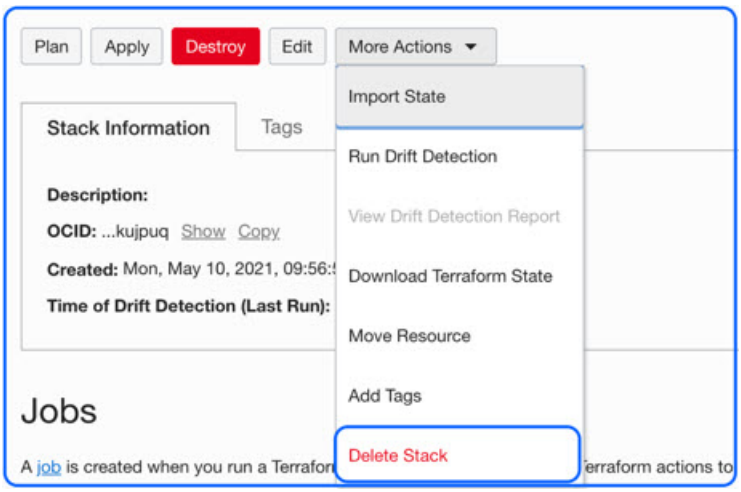
Étape 1 Connectez-vous au portail OCI.

La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.

Étape 2 Choisissez **Developer Services (Services de développeur)** > **Resource Manager (Gestionnaire de ressources)** > **Stack (Pile)**.

Étape 3 Sélectionnez la pile créée par Terraform Template-2, puis cliquez sur **Destroy** (Détruire) dans le menu déroulant **Terraform Actions** (Actions Terraform). La tâche de destruction sera créée, ce qui prendra un certain temps pour supprimer les ressources les unes après les autres.

Étape 4 Une fois la tâche de destruction terminée, vous pouvez supprimer la pile du menu déroulant **More Actions** (Plus d'actions), comme illustré dans la figure ci-dessous.



Après la suppression réussie de la pile Terraform Template-1, vous devez vérifier si toutes les ressources sont supprimées et qu'il n'y a aucun reste.

Supprimer l'évolutivité automatique à l'aide de Cloud Shell

L'utilisateur peut utiliser le script pour supprimer les piles et les fonctions Oracle en exécutant la commande `python3 oci_asav_autoscale_teardown.py` dans l'interface Cloud Shell. Si les piles sont déployées manuellement, mettez à jour l'identifiant de pile de stack1 et stack2, ainsi que l'identifiant de l'application dans le fichier *teardown_parameters.json*.

CHAPITRE 12

Déployer l'ASA virtuel sur Google Cloud Platform

Vous pouvez déployer l'ASA virtuel sur Google Cloud Platform (GCP).

- Aperçu, à la page 255
- Prérequis, à la page 257
- Lignes directrices et limites relatives à la licence, à la page 257
- Exemple de topologie de réseau, à la page 258
- Déployer l'ASA virtuel sur Google Cloud Platform, à la page 259
- Accéder à l'instance ASA virtuel sur GCP, à la page 262
- Utilisation et rapport d'utilisation du processeur (CPU), à la page 265

Aperçu

GCP vous permet de créer, de déployer et de faire évoluer des applications, des sites Web et des services sur la même infrastructure que Google.

L'ASA virtuel exécute le même logiciel que les ASA physiques pour fournir des fonctionnalités de sécurité éprouvées dans un format virtuel. L'ASA virtuel peut être déployé dans le GCP public. Il peut ensuite être configuré pour protéger les charges de travail des centres de données virtuels et physiques qui se développent, se contractent ou changent d'emplacement au fil du temps.

Prise en charge des types de machines GCP

Sélectionnez le type et la taille de machine virtuelle Google qui répondent à vos besoins ASA virtuel.

L'ASA virtuel prend en charge les types de machines GCP *à usage général N1, N2* et *C2 optimisées pour le calcul* :

Tableau 25 : Types de machines optimisées pour le calcul prises en charge

Types de machines optimisées pour le calcul	Attributs	
	vCPU	Mémoire (Go)
c2-standard-4	4	16
c2-standard-8	8	32
c2-standard-16	16	64

Tableau 26 : Types de machines générales prises en charge

Type de machine	Attributs	
	vCPU	Mémoire (Go)
n1-standard-4	4	15
n1-standard-8	8	30
n1-standard-16	16	60
n2-standard-4	4	16
n2-standard-8	8	32
n2-standard-16	16	64
n2-highmem-4	4	32
n2-highmem-8	8	64

- L'ASA virtuel nécessite un minimum de 3 interfaces.
- Le maximum de vCPU pris en charge est de 16.
- Le type de machine à mémoire optimisée n'est pas pris en charge.

Vous créez un compte sur GCP, lancez une instance ASA virtuel à l'aide de l'offre du pare-feu virtuel ASA (ASA virtuel) sur le Marché GCP et choisissez un type de machine GCP.

Limites du type de machine C2 optimisée pour le calcul

Les types de machines C2 optimisées pour le calcul ont les restrictions suivantes :

- Vous ne pouvez pas utiliser de disques persistants régionaux avec des types de machines optimisées pour le calcul. Pour en savoir plus, consultez la documentation de Google Ajout ou redimensionnement de disques persistants régionaux.
- Sous réserve de limites de disque différentes de celles des types de machines à usage général et à mémoire optimisée. Pour en savoir plus, consultez la documentation de Google Bloquer la performance du stockage.
- Disponible uniquement dans certaines zones et régions. Pour plus d'informations, consultez la documentation de Google Régions et zones disponibles.
- Disponible uniquement sur certaines plateformes CPU. Pour plus d'informations, consultez la documentation de Google Plateformes CPU.

Niveaux de performance pour ASA virtuel

L'ASA virtuel prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement.

Niveau de performance	Type d'instance (cœur/RAM)	Limite du débit	Limite de session RA VPN
ASAv5	c2-standard-4 4 cœurs/16 Go	100 Mbit/sec	50
ASAv10	c2-standard-4 4 cœurs/16 Go	1 Gbit/sec	250
ASAv30	c2-standard-4 4 cœurs/16 Go	2 Gbit/s	750
ASAv50	c2-standard-8 8 cœurs/32 Go	7,6 Gbit/s	10 000
ASAv100	c2-standard-16 16 cœurs/64 Go	16 Gbit/s	20 000

Prérequis

- Créez un compte GCP à l'adresse https://cloud.google.com.
- Créez votre projet GCP. Consultez la documentation de Google, Création de votre projet.
- Obtenez une licence pour l'ASA virtuel. Jusqu'à ce que vous obteniez une licence pour l'ASA virtuel, il fonctionnera en mode dégradé, ce qui n'autorisera que 100 connexions et un débit de 100 kbit/s. Consultez Licences : gestion des licences Smart Software.
- Exigences d'interface :
  - Interface de gestion : utilisée pour connecter l'ASA virtuel à ASDM; ne peut pas être utilisée pour le trafic traversant.
  - Interface interne : utilisée pour connecter l'ASA virtuel aux hôtes internes.
  - Interface externe : utilisée pour connecter l'ASA virtuel au réseau public.
- Chemins de communication :
  - Adresses IP publiques pour l'accès à l'ASA virtuel.
- Pour les exigences du système ASA virtuel, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

L'ASA virtuel sur GCP prend en charge les fonctionnalités suivantes :

- Déploiement dans le cloud privé virtuel (VPC) de GCP
- Maximum de 16 vCPU par instance
- Mode avec routeur (par défaut)
- Licences : Seul le protocole BYOL est pris en charge

Fonctionnalités non prises en charge

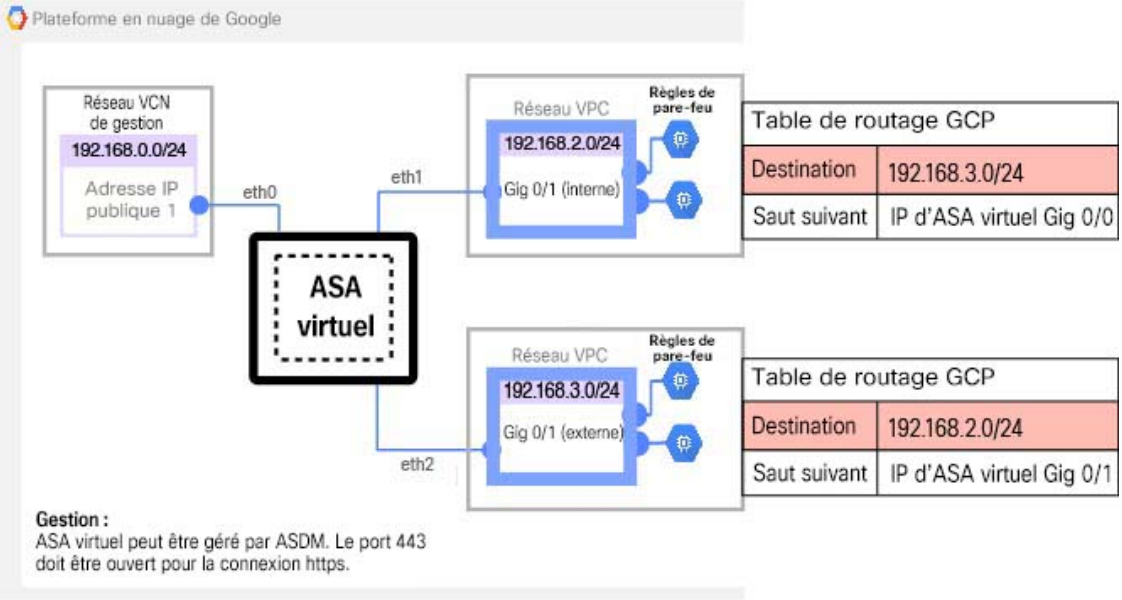
L'ASA virtuel sur GCP ne prend pas en charge les éléments suivants :

- IPv6
  - Le paramètre IPv6 au niveau de l'instance n'est pas pris en charge sur le GCP
  - Seul l'équilibreur de charges peut accepter les connexions IPv6 et les transmettre sur IPv4 aux instances de GCP
- Cadres jumbo
- Haute disponibilité en natif ASA virtuel
- Évolutivité automatique
- Modes transparent/en ligne/passif

Exemple de topologie de réseau

La figure suivante montre la topologie de réseau recommandée pour l'ASA virtuel en mode pare-feu routé avec trois sous-réseaux configurés dans GCP pour l'ASA virtuel (gestion, interne et externe).

Illustration 54 : Exemple d'ASA virtuel sur le déploiement GCP



Déployer l'ASA virtuel sur Google Cloud Platform

Vous pouvez déployer l'ASA virtuel sur Google Cloud Platform (GCP).

Créer des réseaux vPC

Avant de commencer

Le déploiement de ASA virtuel nécessite trois réseaux que vous devez créer avant de déployer l'ASA virtuel. Les réseaux sont les suivants :

- VPC de gestion pour le sous-réseau de gestion.
- VPC interne pour le sous-réseau interne.
- VPC externe pour le sous-réseau externe.

En outre, vous configurez des tableaux de routage et des règles de pare-feu de GCP pour permettre au trafic de circuler dans l'ASA virtuel. Les tableaux de routage et les règles de pare-feu sont distincts de ceux configurés sur l'ASA virtuel lui-même. Nommez les tableaux de routage et les règles de pare-feu de GCP en fonction du réseau et des fonctionnalités associés. Consultez Exemple de topologie de réseau, à la page 258.

Procédure

Étape 1 Dans la console GCP, choisissez **Networking (réseautage)** > **VPC network (réseau VPC)** > **VPC networks (réseaux VPC)**, puis cliquez sur **Create VPC Network** (créer un réseau VPC).

Étape 2 Dans le champ **Name** (nom), saisissez le nom descriptif de votre réseau VPC, par exemple, *vpc-asiasouth-mgmt*.

Étape 3 Dans le **Subnet creation mode** (mode de création de sous-réseau), cliquez sur **Custom** (personnalisé).

Étape 4 Dans le champ **Name** (nom) sous **New subnet** (nouveau sous-réseau), saisissez le nom souhaité, par xemple, *vpc-asiasouth-mgmt*.

Étape 5 Dans la liste déroulante **Region** (région), sélectionnez la région appropriée pour votre déploiement. Les trois réseaux doivent se trouver dans la même région.

Étape 6 Dans le champ **IP address range** (plage d'adresses IP), saisissez le sous-réseau du premier réseau au format CIDR, par exemple 10.10.0.0/24.

Étape 7 Acceptez les valeurs par défaut de tous les autres paramètres, puis cliquez sur **Create** (Créer).

Étape 8 Répétez les étapes 1 à 7 pour créer les deux autres réseaux VPC.

Créer les règles de pare-feu

Vous appliquez les règles de pare-feu de l'interface de gestion (pour autoriser les connexions SSH et HTTPS) lors du déploiement de l'instance ASA virtuel, consultez Créer l'instance ASA virtuel sur GCP, à la page 260. Selon vos besoins, vous pouvez également créer des règles de pare-feu pour les interfaces interne et externe.

Procédure

Étape 1 Dans la console GCP, choisissez **Networking (réseautage)** > **VPC network (réseau VPC)** > **Firewall (pare-feu)**, puis cliquez sur **Create Firewall Rule** (créer une règle de pare-feu).

Étape 2 Dans le champ **Name** (nom), saisissez un nom descriptif pour votre règle de pare-feu, par exemple, *vpc-asiasouth-inside-fwrule*.

Étape 3 Dans la liste déroulante **Network** (réseau), sélectionnez le nom du réseau VPC pour lequel vous créez la règle de pare-feu, par exemple, *asav-south-inside*.

Étape 4 Dans la liste déroulante **Targets** (cibles), sélectionnez l'option applicable à votre règle de pare-feu, par exemple, **All instances in the network** (toutes les instances du réseau).

Étape 5 Dans le champ **Source IP ranges** (plages IP sources), saisissez les plages d'adresses IP sources au format CIDR, par exemple, 0.0.0.0/0.

Le trafic n'est autorisé que par des sources comprises dans ces plages d'adresses IP.

Étape 6 Sous **Protocols and ports** (protocoles et ports), sélectionnez **Specified protocols and ports** (protocoles et ports spécifiés).

Étape 7 Ajoutez vos règles de sécurité.

Étape 8 Cliquez sur **Create** (créer).

Créer l'instance ASA virtuel sur GCP

Effectuez les étapes suivantes pour déployer une instance ASA virtuel en utilisant l'offre de pare-feu virtuel Cisco ASA (ASA virtuel) du Marché GCP.

Procédure

Étape 1 Connectez-vous à la console GCP.

Étape 2 Cliquez sur **Navigation menu (Menu de navigation)** > **Marketplace (Marché)**.

Étape 3 Effectuez une recherche sur le Marché pour « Cisco ASA virtual firewall (ASAv) » (Pare-feu virtuel Cisco ASA (ASAv)) et choisissez l'offre.

Étape 4 Cliquez sur **Launch** (Lancer).

Étape 5 Ajoutez un **Deployment name** (Nom de déploiement) unique pour l'instance.

Étape 6 Sélectionnez la **Zone** dans laquelle vous souhaitez déployer l'ASA virtuel.

Étape 7 Sélectionnez le **Machine type** (Type de machine) approprié. Pour obtenir la liste des types de machines prises en charge, consultez Aperçu, à la page 255.

Étape 8 (Facultatif) Collez la clé publique de la paire de clés SSH sous **SSH key (optional)** (Clé SSH (facultatif)).

La paire de clés se compose d'une clé publique que GCP stocke et d'un fichier de clé privée que l'utilisateur stocke. Ensemble, ils vous permettent de vous connecter à votre instance en toute sécurité. Assurez-vous d'enregistrer la paire de clés à un emplacement connu, car elle devra se connecter à l'instance.

Étape 9 Choisissez d'autoriser ou de bloquer les clés SSH à l'échelle du projet pour l'accès à cette instance. Consultez la documentation de Google Autoriser ou bloquer les clés SSH publiques à l'échelle du projet à partir d'une instance Linux.

Étape 10 (Facultatif) Sous **Startup script** (Script de démarrage), fournissez la configuration day0 (jour0) pour votre ASA virtuel. La configuration day0 (jour0) est appliquée lors du premier démarrage d'ASA virtuel.

L'exemple suivant montre une configuration day0 (jour0) que vous pouvez copier et coller dans le champ **Startup script** (Script de démarrage) :

Consultez les Guides de configuration ASA et la Référence sur les commandes ASA pour en savoir plus sur les commandes ASA.

Important
Lorsque vous copiez du texte à partir de cet exemple, vous devez valider le script dans un éditeur de texte ou un moteur de validation tiers pour éviter les erreurs de format et supprimer les caractères Unicode non valides.

```
!ASA Version 9.15.1

interface management0/0

management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 60
ssh version 2
username admin password cisco123 privilege 15
username admin attributes
```

```
service-type admin
! required config end
dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
```

Étape 11 Conservez le **Boot disk type** (Type de disque de démarrage) par défaut et la **Boot disk size in GB** (Taille de disque de démarrage en Go) pour l'espace disque provisionné.

Étape 12 Configurez les interfaces sous **Network interfaces** (Interfaces réseau).

- gestion
- interne
- externe

Remarque
Vous ne pouvez pas ajouter des interfaces à une instance après l'avoir créée. Si vous créez l'instance avec une configuration d'interface incorrecte, vous devez supprimer l'instance et la recréer avec la configuration d'interface appropriée.

a) Dans la liste déroulante **Network** (Réseau), sélectionnez un réseau VPC, par exemple, *vpc-asiasouth-mgmt*.
b) Dans la liste déroulante **External IP** (Adresse IP externe), sélectionnez l'option appropriée.

Pour l'interface de gestion, sélectionnez **External IP** (Adresse IP externe) à **Ephemeral** (Éphémère). Cette opération est facultative pour les interfaces interne et externe.

c) Cliquez sur **Done (Terminé)**.

Étape 13 Appliquez les règles de pare-feu sous **Firewall** (Pare-feu).

- Cochez la case **Allow TCP port 22 traffic from the Internet (SSH access)** (Autoriser le trafic du port TCP 22 de l'Internet (accès SSH)) pour autoriser SSH.
- Cochez la case **Allow HTTPS traffic from the Internet (ASDM access)** (Autoriser le trafic HTTPS de l'Internet (accès ASDM)) pour autoriser les connexions HTTPS.

Étape 14 Cliquez sur **More** (Plus) pour développer l'affichage et assurez-vous que **IP Forwarding** (Transfert IP) est défini sur **On** (Activé).

Étape 15 Cliquez sur **Deploy** (Déployer).

Affichez les détails de l'instance dans la page d'instance de VM de la console GCP. Vous trouverez l'adresse IP interne, l'adresse IP externe et les contrôles pour arrêter et démarrer l'instance. Vous devez arrêter l'instance si vous devez la modifier.

Accéder à l'instance ASA virtuel sur GCP

Assurez-vous d'avoir déjà activé une règle de pare-feu pour autoriser les connexions SSH (TCP par le port 22) pendant le déploiement. Consultez Créer l'instance ASA virtuel sur GCP, à la page 260 pour de plus amples renseignements.

Cette règle de pare-feu active l'accès à l'instance ASA virtuel et vous permet de vous connecter à l'instance en utilisant les méthodes suivantes.

- External IP (IP externe)
  - Tout autre outil client SSH ou tiers
- Console de série
- Ligne de commande Gcloud

Consultez la documentation de Google, Connexion aux instances pour en savoir plus.

Remarque Vous pouvez vous connecter à l'instance ASA virtuel en utilisant les renseignements d'authentification spécifiés dans la configuration day0 (jour0) ou en utilisant la paire de clés SSH que vous avez créée lors du lancement de l'instance.

Se connecter à l'instance ASA virtuel à l'aide d'une adresse IP externe

L'instance ASA virtuel se voit attribuer une adresse IP interne et une adresse IP externe. Vous pouvez utiliser l'adresse IP externe pour accéder à l'instance ASA virtuel.

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

Étape 2 Cliquez sur le nom de l'instance ASA virtuel pour ouvrir la page **VM instance details** (Détails de l'instance de VM).

Étape 3 Sous l'onglet **Details** (Détails), cliquez sur le menu déroulant du champ **SSH**.

Étape 4 Sélectionnez l'option souhaitée dans le menu déroulant **SSH**.

Vous pouvez vous connecter à l'instance ASA virtuel en utilisant la méthode suivante.

- Tout autre outil client SSH ou tiers : consultez l'information sur la connexion à l'aide d'outils tiers de la documentation de Google pour en savoir plus.

Remarque
Vous pouvez vous connecter à l'instance ASA virtuel en utilisant les renseignements d'authentification spécifiés dans la configuration day0 (jour0) ou en utilisant la paire de clés SSH que vous avez créée lors du lancement de l'instance.

Se connecter à l'instance ASA virtuel à l'aide de SSH

Pour vous connecter à l'instance ASA virtuel à partir d'un système de type Unix, connectez-vous à l'instance à l'aide de SSH.

Procédure

Étape 1 Utilisez la commande suivante pour définir les autorisations de fichier afin que seul vous puissiez lire le fichier :

```
$ chmod 400 <private_key>
```

Lieu :

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

Étape 2 Utilisez la commande SSH suivante pour accéder à l'instance.

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

Lieu :

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

`<username>` correspond au nom d'utilisateur pour l'instance ASA virtuel.

`<public-ip-address>` correspond à l'adresse IP publique de votre instance que vous avez extraite de la console.

Se connecter à l'instance ASA virtuel à l'aide de la console de série

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

Étape 2 Cliquez sur le nom de l'instance ASA virtuel pour ouvrir la page **VM instance details** (Détails de l'instance de VM).

Étape 3 Sous l'onglet **Details** (Détails), cliquez sur **Connect to serial console** (Se connecter à la console série).

Consultez la documentation de Google, Interagir avec la console série pour en savoir plus.

Se connecter à l'instance ASA virtuel à l'aide de GCloud

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

Étape 2 Cliquez sur le nom de l'instance ASA virtuel pour ouvrir la page **VM instance details** (Détails de l'instance de VM).

Étape 3 Sous l'onglet **Details** (Détails), cliquez sur le menu déroulant du champ **SSH**.

Étape 4 Cliquez sur **View gcloud command (Voir la commande gcloud)** > **Run in Cloud Shell (Exécuter dans Cloud Shell)**.

La fenêtre de terminal Cloud Shell s'ouvre. Consultez la documentation de Google, Présentation de l'outil de ligne de commande gcloudet Calcul gcloud ssh pour en savoir plus.

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 sur environ 30 à 40 % de la capacité totale du processeur en dehors des heures de pointe et sur environ 60 à 70 % de capacité pendant les heures de pointe.

Utilisation de vCPU dans ASA virtuel

L'utilisation du vCPU ASA virtuel affiche la quantité de vCPU utilisée pour le chemin de données, le point de contrôle et les processus externes.

L'utilisation du vCPU signalé par GCP comprend l'utilisation de l'ASA virtuel, comme décrit :

- Délai d'inactivité d'ASA virtuel
- %SYS surdébit utilisé pour la machine 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

La commande **show cpu usage** (afficher l'utilisation du processeur) peut être utilisée pour afficher les statistiques d'utilisation du processeur.

Exemple

```
Ciscoasa#show cpu usage

Utilisation du processeur pendant 5 secondes = 1 %; 1 minute : 2 %; 5 minutes : 1 %
```

Voici un exemple dans lequel l'utilisation de vCPU signalée est sensiblement différente :

- Rapports ASA virtuel : 40 %
- DP : 35 %
- Processus externes : 5 %
- 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.

Rapport d'utilisation du processeur (CPU) de GCP

Cliquez sur le nom de l'instance sur la console GCP, puis sur l'onglet **Monitoring (**supervision). Vous pourrez voir le pourcentage d'utilisation du processeur (CPU).

Compute Engine vous permet d'exporter des rapports détaillés de votre utilisation de Compute Engine vers un compartiment de stockage Google Cloud à l'aide de la fonctionnalité d'exportation de l'utilisation. Les rapports d'utilisation fournissent des renseignements sur la durée de vie de vos ressources. Par exemple, vous pouvez voir le nombre d'instances de machine virtuelle de votre projet qui exécutent un type de machine `n2-standard-4` et la durée de l'exécution de chaque instance. Vous pouvez également passer en revue l'espace de stockage d'un disque persistant et des informations sur d'autres fonctionnalités de Compute Engine.

Graphiques ASA virtuel et GCP

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et le GCP :

- Les numéros de graphique GCP sont toujours supérieurs aux numéros d'ASA virtuel.
- GCP l'appelle « %CPU usage »; l'ASA virtuel l'appelle « %CPU utilization ».

Les termes « %CPU utilization » et « %CPU usage » signifient des choses différentes :

- L'utilisation du CPU fournit des statistiques sur les processeurs (CPU) physiques.
- L'usage du CPU fournit des statistiques pour les processeurs (CPU) logiques, qui sont basées sur l'hyperthreading du CPU. Comme un seul processeur virtuel (vCPU) est utilisé, l'hyperthreading n'est pas activé.

GCP calcule le pourcentage d'usage du CPU comme suit :

Nombre de 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

CHAPITRE 13

Déployer la solution d'évolutivité automatique de l'ASA virtuel sur GCP

- Aperçu, à la page 267
- Télécharger le paquet de déploiement, à la page 269
- Composants de la solution d'évolutivité automatique, à la page 269
- Prérequis, à la page 272
- Déployer la solution d'évolutivité automatique, à la page 279
- Logique d'évolutivité automatique, à la page 283
- Journalisation et débogage, à la page 284
- Lignes directrices et limites relatives à la licence, à la page 285
- Dépannage, à la page 286

Aperçu

Les sections suivantes décrivent comment les composants de la solution d'évolutivité automatique fonctionnent pour la ASA virtuel sur GCP.

À propos de la solution d'évolutivité automatique

L'évolutivité automatique d'ASA virtuel pour GCP est une implémentation complète sans serveur qui utilise l'infrastructure sans serveur fournie par GCP (fonctions dans le nuage, équilibreurs de charges, publication/abonnement, groupes d'instances, etc.).

Certaines des fonctionnalités clés de l'évolutivité automatique d'ASA virtuel pour l'implémentation GCP comprennent :

- Déploiement basé sur le modèle de gestionnaire de déploiement GCP.
- Prise en charge des mesures d'évolutivité en fonction du CPU.
- Prise en charge du déploiement d'ASA virtuel et des zones de multi-disponibilité.
- La configuration entièrement automatisée s'applique automatiquement aux instances ASA virtuel soumise à l'évolutivité à la hausse.
- Prise en charge des équilibreurs de charges et des zones de multi-disponibilité.

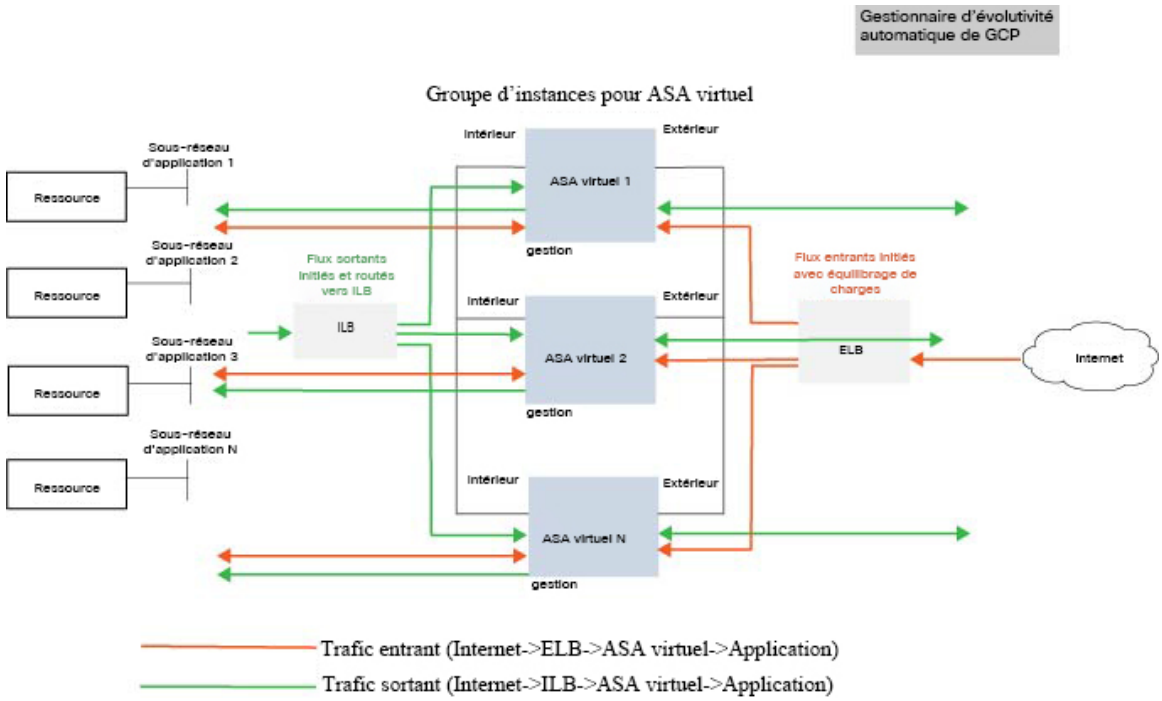
- Cisco fournit un paquet de déploiement de l'évolutivité automatique pour GCP afin de faciliter le déploiement.

Scénario d'évolutivité automatique

L'évolutivité automatique d'ASA virtuel pour GCP est une solution d'évolutivité horizontale automatisée qui positionne un groupe d'instances ASA virtuel entre un équilibreur de charge interne (ILB) et un équilibreur de charge externe (ELB) GCP.

- L'ELB distribue le trafic Internet aux instances ASA virtuel du groupe d'instances; le pare-feu transfère ensuite le trafic à l'application.
- L'ILB distribue le trafic Internet sortant d'une application aux instances ASA virtuel du groupe d'instances; le pare-feu transfère ensuite le trafic à Internet.
- Un paquet réseau ne traversera jamais les deux équilibreurs de charges (interne et externe) en une seule connexion.
- Le nombre d'instances ASA virtuel dans l'ensemble d'évolutivité se verra évoluer et sera configuré automatiquement en fonction des conditions de charge.

Illustration 55 : Scénario d'évolutivité automatique d'ASA virtuel



Champ d'application

Ce document couvre les procédures détaillées pour déployer les composants sans serveur pour la solution ASA virtuel d'évolutivité automatique pour GCP.

Important

- Lisez le document entier avant de commencer le déploiement.
- Assurez-vous que les conditions préalables sont remplies avant de commencer le déploiement.
- Assurez-vous de suivre les étapes et l'ordre d'exécution décrits dans le présent document.

Télécharger le paquet de déploiement

La solution d'évolutivité automatique d'ASA virtuel pour GCP est un déploiement basé sur le modèle de gestionnaire de déploiement GCP qui utilise l'infrastructure sans serveur fournie par GCP (fonctions dans le nuage, équilibreurs de charges, publication/abonnement, groupes d'instances, etc.).

Téléchargez les fichiers requis pour lancer la solution d'évolutivité automatique d'ASA virtuel pour GCP. Les scripts et les modèles de déploiement pour votre version ASA sont disponibles dans le référentiel GitHub.

Attention Remarque : les scripts et les modèles de déploiement fournis par Cisco pour l'évolutivité automatique sont présentés à titre d'exemples de code source libre et ne font pas l'objet de l'assistance technique du TAC dans sa portée normale.

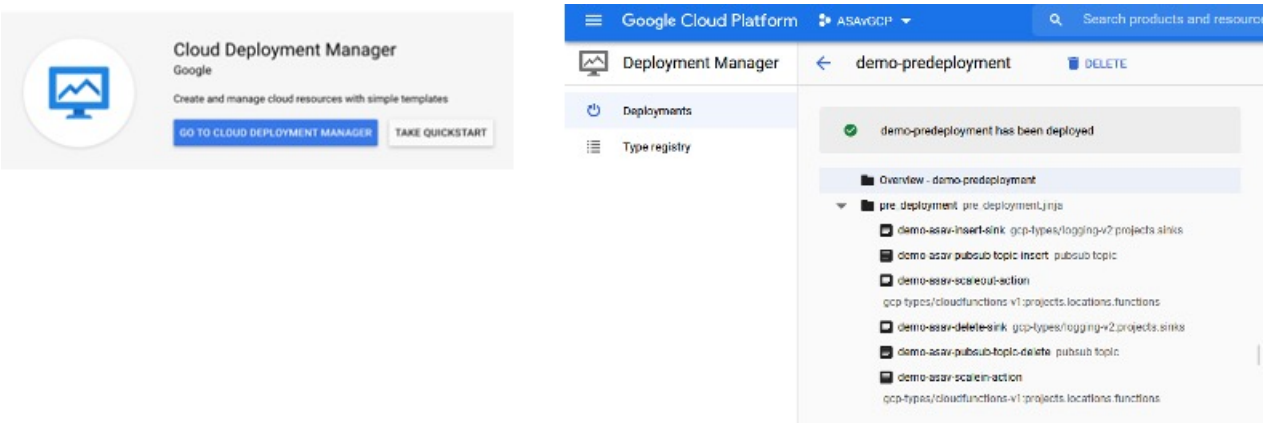
Composants de la solution d'évolutivité automatique

Les composants suivants constituent la solution d'évolutivité automatique ASA virtuel pour GCP.

Gestionnaire de déploiement

- Traitez votre configuration comme du code et effectuez des déploiements reproductibles. Google Cloud Deployment Manager vous permet de spécifier toutes les ressources nécessaires à votre application dans un format explicite à l'aide de YAML. Vous pouvez également utiliser des modèles Python ou Jinja2 pour paramétrer la configuration et permettre la réutilisation des schémas de déploiement courants.
- Créez des fichiers de configuration qui définissent les ressources. Le processus de création de ces ressources peut être répété à plusieurs reprises avec des résultats cohérents. Consultez https://cloud.google.com/deployment-manager/docs pour de plus amples renseignements.

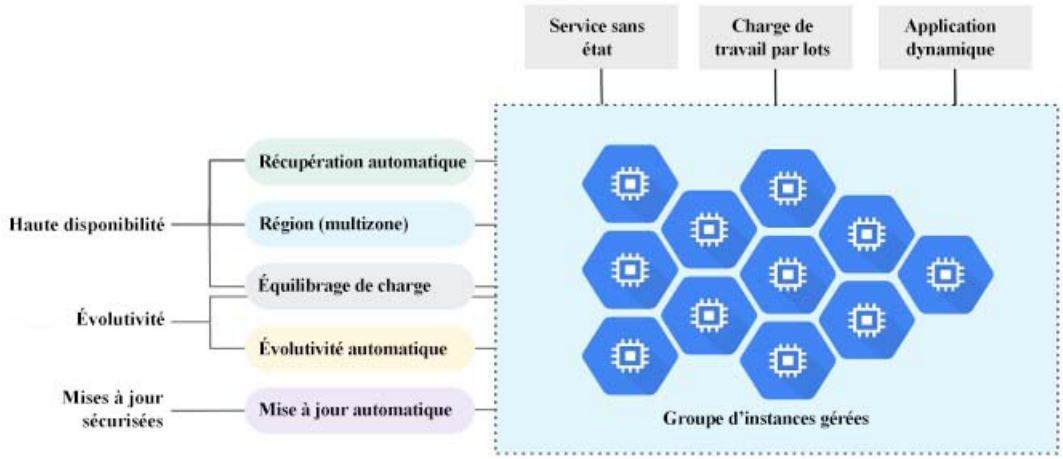
Illustration 56 : Vue du gestionnaire de déploiement



Groupe d'instances gérées dans GCP

Un groupe d'instances gérées (MIG) crée chacune de ses instances gérées en fonction du modèle d'instance et de la configuration dynamique facultative que vous spécifiez. Consultez https://cloud.google.com/compute/docs/instance-groups pour de plus amples renseignements.

Illustration 57 : Fonctionnalités du groupe d'instances

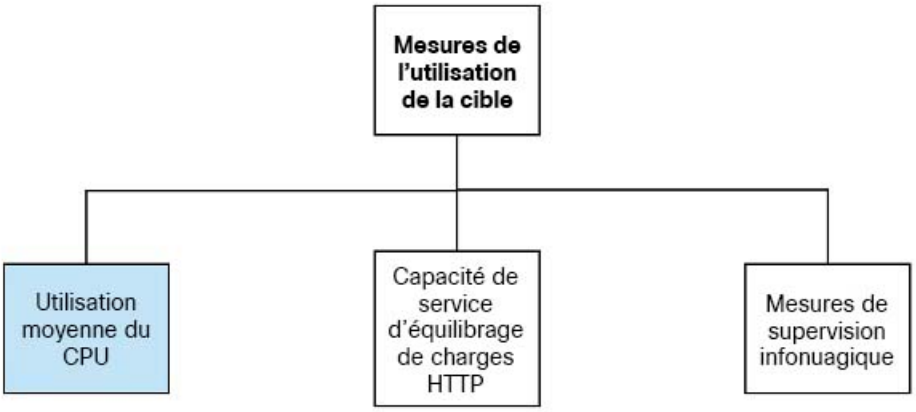


Mesures de l'utilisation de la cible

- Le diagramme suivant présente les mesures d'utilisation de la cible. Seules les mesures d'utilisation moyenne du CPU sont utilisées pour prendre des décisions en matière d'évolutivité automatique.
- Le dispositif d'évolutivité automatique recueille en permanence des renseignements sur l'utilisation en fonction de la mesure d'utilisation sélectionnée, compare l'utilisation réelle à votre utilisation cible souhaitée et utilise ces renseignements pour déterminer si le groupe doit supprimer des instances (évolutivité à la baisse) ou ajouter des instances (évolutivité à la hausse).

- Le niveau d'utilisation cible est le niveau auquel vous souhaitez maintenir vos instances de machine virtuelle (VM). Par exemple, si vous évoluez en fonction de l'utilisation du CPU, vous pouvez définir votre niveau d'utilisation cible à 75 % et le dispositif d'évolutivité automatique maintiendra l'utilisation du CPU du groupe d'instances spécifié à 75 %. Le niveau d'utilisation de chaque mesure est interprété différemment en fonction de la politique d'évolutivité automatique. Consultez https://cloud.google.com/compute/docs/autoscaler pour de plus amples renseignements.

Illustration 58 : Mesures de l'utilisation de la cible



Fonctions de nuage sans serveur

Vous utilisez les fonctions Google Cloud sans serveur pour définir le mot de passe SSH, activer le mot de passe et modifier le nom de domaine lorsque l'instance se présente dans le gestionnaire de groupe d'instances.

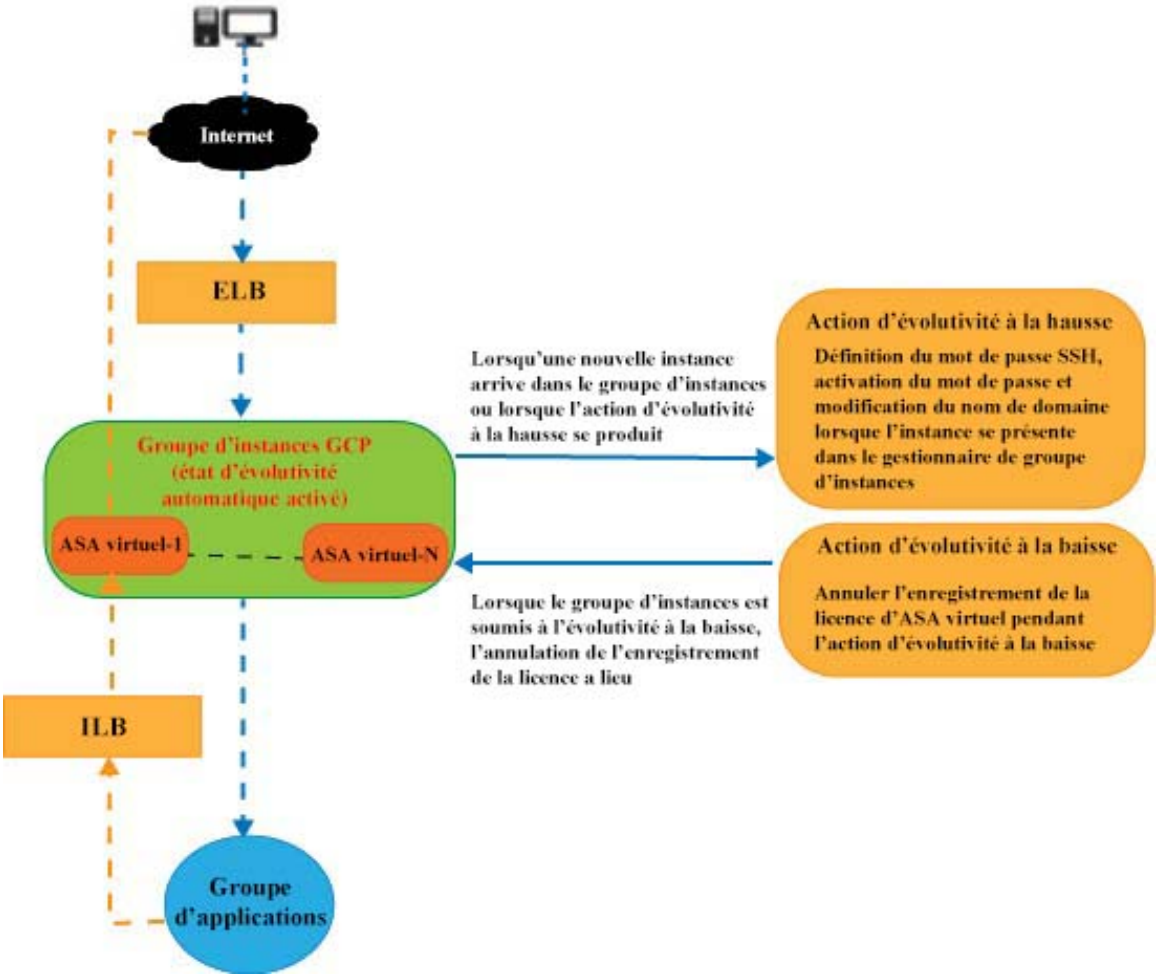
- Lorsqu'une nouvelle instance ASA virtuel apparaît dans le groupe d'instances lors du processus d'évolutivité à la hausse, vous devez définir le mot de passe SSH, activer le mot de passe et changer le nom de domaine, car vous ne pouvez pas toujours surveiller le processus d'évolutivité à la hausse.
- Les fonctions du nuage sont déclenchées par un sujet de publication ou d'abonnement en nuage pendant le processus d'évolutivité à la hausse. Vous disposez également d'un récepteur de journaux avec un filtre exclusif à l'ajout d'instances lors de l'évolutivité à la hausse.

Annulation de l'enregistrement de la licence sans serveur à l'aide des fonctions du nuage

- Pendant que les instances sont supprimées lors de l'évolutivité à la baisse, vous devez annuler l'enregistrement de la licence de l'instance ASA virtuel.
- Les fonctions du nuage sont déclenchées par un sujet de publication ou d'abonnement en nuage. En particulier pour le processus de suppression, vous disposez d'un récepteur de journaux avec un filtre exclusif à la suppression des instances lors de l'évolutivité à la baisse.
- La fonction du nuage, lorsqu'elle est déclenchée, se connecte en SSH à l'instance ASA virtuel à supprimer et exécute la commande pour annuler l'enregistrement de la licence.

Présentation générale de la solution d'évolutivité automatique

Illustration 59 : Présentation de la solution d'évolutivité automatique



Prérequis

Ressources GCP

Projet GCP

Un projet existant ou nouvellement créé est requis pour déployer tous les composants de cette solution.

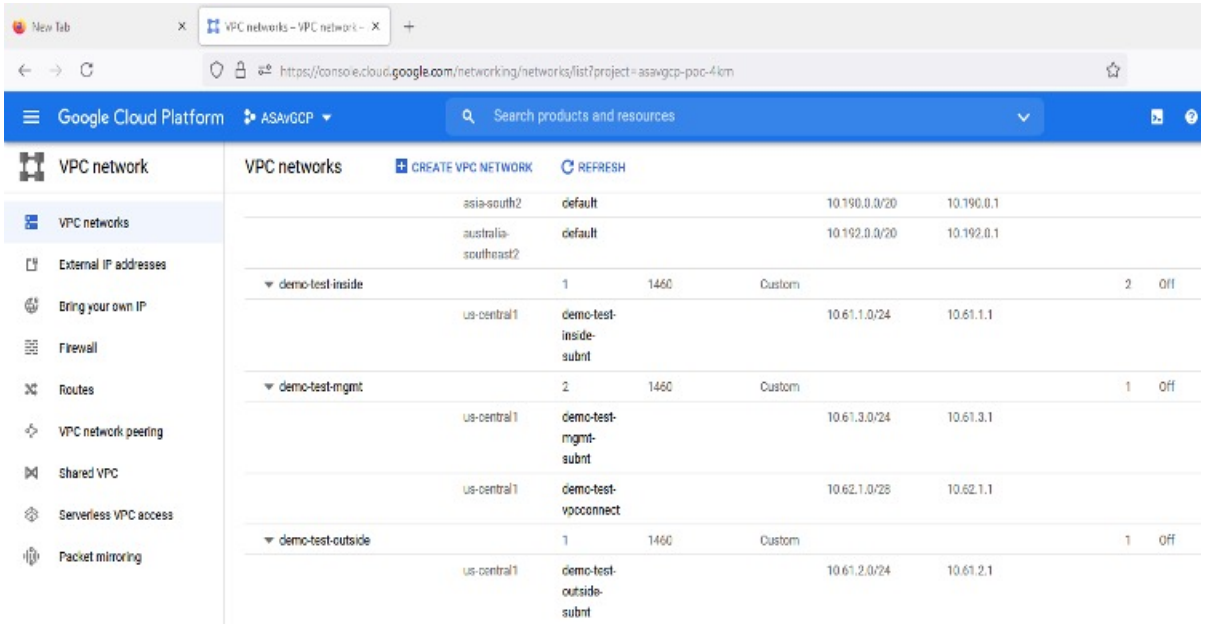
Mise en réseau

Assurez-vous que trois VPC sont disponibles ou créés. Un déploiement de l'évolutivité automatique ne créera, ne modifiera ni ne gérera de ressources réseau.

L'ASA virtuel nécessite trois interfaces réseau, donc votre réseau virtuel nécessite trois sous-réseaux pour :

- Le trafic de gestion
- Le trafic interne
- Le trafic externe

Illustration 60 : Vue du réseau VPC



Pare-feu

Des règles de pare-feu qui permettent la communication inter-VPC et permettent également la création de sondes d'intégrité. Vous devez noter les balises de pare-feu utilisées plus tard dans le modèle de gestionnaire de déploiement.

Les ports suivants doivent être ouverts dans le groupe de sécurité réseau auquel les sous-réseaux sont connectés :

- SSH (TCP/22) : requis pour la sonde d'intégrité entre l'équilibreur de charges et l'ASA virtuel. Requis pour la communication entre les fonctions sans serveur et l'ASA virtuel.
- Protocole/ports spécifiques à l'application : requis pour toutes les applications des utilisateurs (par exemple, TCP/80, etc.).

Préparer le fichier de configuration ASA

Préparez un fichier de configuration ASA virtuel qui sera ajouté dans le fichier de configuration jinja du gestionnaire de déploiement. Cette configuration sera utilisée comme script de démarrage dans le modèle d'instance pour ASA virtuel dans le projet.

Le fichier de configuration doit comporter au moins les éléments suivants :

- Définissez l'attribution d'adresse IP DHCP pour toutes les interfaces.
- Nic0 doit être marqué comme « outside » (externe), car l'équilibreur de charges GCP transfère le trafic uniquement à nic0.

- Nic0 sera utilisé pour SSH vers ASA virtuel, car il prend uniquement en charge le transfert IP.
- Activez SSH sur l'interface externe dans la configuration ASA.
- Créez une configuration NAT pour transférer le trafic de l'interface externe vers l'interface interne.
- Créez un protocole d'accès pour autoriser le trafic souhaité.
- Pour l'état d'intégrité des ressources, leurs sondes d'intégrité doivent être redirigées vers le serveur de métadonnées à l'aide des règles NAT appropriées.

Voici un exemple de fichier de configuration ASA pour référence uniquement.

```
!ASA Version 9.15.1.10
!Interface Config
interface G0/0
nameif inside
security-level 100
ip address dhcp setroute
no shutdown


interface G0/1
nameif management
security-level 50
ip address dhcp setroute
no shutdown

interface M0/0
no management-only
nameif outside
security-level 0
ip address dhcp setroute
no shutdown
!
same-security-traffic permit inter-interface
!
!Due to some constraints in GCP,
!"GigabitEthernet0/0" will be used as a Management interface
!"Management0/0" will be used as a data interface
crypto key generate rsa modulus 2048
ssh 0.0.0.0 0.0.0.0 management
ssh version 2
ssh timeout 60
aaa authentication ssh console LOCAL
ssh authentication publickey {{ properties["publicKey"] }}
username admin privilege 15
username admin attributes
service-type admin

! required config end
dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
!
access-list all extended permit ip any any
access-list out standard permit any4
access-group all global
! Objects
object network metadata
host 169.254.169.254
object network ilb
host $(ref.{{ properties["resourceNamePrefix"] }}-ilb-ip.address)
```

```
object network hc1
subnet 35.191.0.0 255.255.0.0
object network hc2
subnet 130.211.0.0 255.255.63.0
object network elb
host $(ref.{{ properties["resourceNamePrefix"] }}-elb-ip.address)
object network appServer
host 10.61.2.3
object network defaultGateway
subnet 0.0.0.0 0.0.0.0
! Nat Rules
nat (inside,outside) source dynamic hc1 ilb destination static ilb metadata
nat (inside,outside) source dynamic hc2 ilb destination static ilb metadata
nat (inside,outside) source dynamic defaultGateway interface
 !
 object network appServer
nat (inside,outside) static $(ref.{{ properties["resourceNamePrefix"] }}-elb-ip.address)
object network defaultGateway
nat (outside,inside) dynamic interface
! Route Add
route inside 0.0.0.0 0.0.0.0 10.61.1.1 2
route management 0.0.0.0 0.0.0.0 10.61.3.1 3
license smart register idtoken <licenseIDToken>
```

Créer le paquet de fonction en nuage de GCP

La solution d'évolutivité automatique GCP d'ASA virtuel nécessite que vous créiez deux fichiers d'archive qui fournissent les fonctions en nuage sous la forme d'un paquet ZIP compressé.

- `scalein-action.zip`
- `scaleout-action.zip`

Consultez les instructions de déploiement de l'évolutivité automatique pour savoir comment créer les paquets `scalein-action.zip` et `scaleout-action.zip`.

Ces fonctions sont aussi distinctes que possible pour effectuer des tâches spécifiques et peuvent être mises à niveau au besoin pour améliorer et prendre en charge les nouvelles versions.

Paramètres d'entrée

Le tableau suivant définit les paramètres du modèle et fournit un exemple. Une fois que vous avez choisi ces valeurs, vous pouvez utiliser ces paramètres pour créer le périphérique ASA virtuel lorsque vous déployez le modèle de gestionnaire de déploiement GCP dans votre projet GCP.

Tableau 27 : Paramètres du modèle

Nom du paramètre	Valeurs/Type autorisés	Description	Type de création de ressource
resourceNamePrefix	Chaîne	Toutes les ressources sont créées avec un nom contenant ce préfixe. Exemple : demo-test	New (Nouvelle)

Nom du paramètre	Valeurs/Type autorisés	Description	Type de création de ressource
region	Régions valides prises en charge par GCP [Chaîne]	Nom de la région où le projet sera déployé. Exemple : us-central1	
serviceAccountMailId	Chaîne [ID de courriel]	Adresse courriel qui identifie le compte de service.	
vpcConnectorName	Chaîne	Nom du connecteur qui gère le trafic entre votre environnement sans serveur et votre réseau VPC. Exemple : demo-test-vpc-connector	
bucketName	Chaîne	Nom du compartiment de stockage GCP dans lequel le progiciel ZIP de la fonction en nuage sera chargé. Exemple : demo-test-bkt	
cpuUtilizationTarget	Décimal (0, 1]	L'utilisation moyenne du CPU des machines virtuelles du groupe d'instances que l'évolutivité automatique doit maintenir. Exemple : 0.5	
healthCheckFirewallRuleName	Chaîne	Balise de la règle de pare-feu qui autorise les paquets des plages d'adresses IP de sonde de vérification de l'intégrité. Exemple : demo-test-healthallowall	Existant
insideFirewallRuleName	Chaîne	Balise des règles de pare-feu qui permet la communication dans le VPC interne. Exemple : demo-test-inside- allowall	Existant

Nom du paramètre	Valeurs/Type autorisés	Description	Type de création de ressource
insideVPCName	Chaîne	Nom du VPC interne. Exemple : demo-test-inside	Existant
insideVPCSubnet	Chaîne	Nom du sous-réseau interne. Exemple : demo-test-inside-subnt	Existant
machineType	Chaîne	Type de machine pour la machine virtuelle ASA virtuel. Exemple : e2-standard-4	
maxASAcount	Nombre entier	Le nombre maximal d'instances ASA virtuel autorisées dans le groupe d'instances. Exemple : 3	
mgmtFirewallRuleName	Chaîne	Balise des règles de pare-feu qui permet la communication dans le VPC de gestion. Exemple : demo-test-mgmt- allowall	
mgmtVPCName	Chaîne	Nom du VPC de gestion. Exemple : demo-test-mgmt	
mgmtVPCSubnet	Chaîne	Nom du sous-réseau de gestion. Exemple : demo-test-mgmt-subnt	
minASACount	Nombre entier	Le nombre minimal d'instances ASA virtuel disponibles dans le groupe d'instances à tout moment. Exemple : 1	

Nom du paramètre	Valeurs/Type autorisés	Description	Type de création de ressource
outsideFirewallRuleName	Chaîne	Balise des règles de pare-feu qui permet la communication dans le VPC externe. Exemple : demo-test-outside-allowall	
outsideVPCName	Chaîne	Nom du VPC externe. Exemple : demo-test-outside	
outsideVPCSubnet	Chaîne	Nom du sous-réseau externe. Exemple : demo-test-outside-subnt	
publicKey	Chaîne	Clé SSH de la machine virtuelle ASA virtuel.	
sourceImageURL	Chaîne	Image de l'ASA virtuel qui doit être utilisé dans le projet. Exemple : https://www.googleapis.com/compute/v1/projects/cisco-public/global/images/cisco-asav-9-15-1-15	
Adresse IP du serveur d'applications	Chaîne	Adresse IP interne de la machine Linux interne. Exemple : 10.61.1.2	
Adresse IP de la passerelle du VPC interne	Chaîne	Passerelle du VPC interne. Exemple : 10.61.1.1	
Adresse IP de la passerelle du VPC de gestion	Chaîne	Passerelle du VPC de gestion. Exemple : 10.61.3.1	

Déployer la solution d'évolutivité automatique

Procédure

Étape 1 Copiez le référentiel Git dans un dossier local.

```
git clone git_url -b branch_name
```

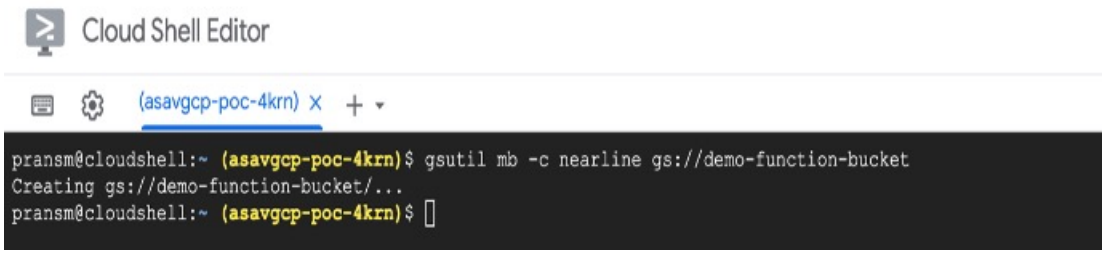
Exemple :

```
Last login: Thu Jun  3 13:01:32 on ttys002
(base) pransm@PRANSM-M-F9KA ~ % git clone https://bitbucket-eng-bgl1.cisco.com/bitbucket/scm/vcb/cloud_autoscale.git -b saaarwar_asa_autoscale_public_key
Cloning into 'cloud_autoscale'...
remote: Enumerating objects: 1604, done.
remote: Counting objects: 100% (1604/1604), done.
remote: Compressing objects: 100% (1507/1507), done.
remote: Total 1604 (delta 759), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (1604/1604), 58.35 MiB | 8.54 MiB/s, done.
Resolving deltas: 100% (759/759), done.
(base) pransm@PRANSM-M-F9KA ~ %
```

Étape 2 Créez le compartiment dans l'interface de ligne de commande gcloud.

```
gsutil mb -c nearline gs://bucket_name
```

Exemple :



Étape 3 Créez des paquets zip compressés :

a) Créez des paquets zip compressés contenant les fichiers suivants à partir des dossiers `scalein_action` et `scaleout_action`.

- main.py
- basic_functions.py

requirements.txt

b) Renommez les paquets zip compressés en `scaleout-action.zip` et `scalein-action.zip`.

Remarque
Naviguez dans le dossier, sélectionnez les fichiers, cliquez avec le bouton droit et sélectionnez « compress | archive » (compresser | archiver) pour créer un fichier .zip que GCP peut lire.

Étape 4 Chargez les paquets zip compressés (`scaleout-action.zip` et `scalein-action.zip`) dans l'espace de travail de l'éditeur en nuage.

Étape 5 Chargez les fichiers suivants du modèle de gestionnaire de déploiement dans l'espace de travail de l'éditeur en nuage.

- asav_autoscale.jinja
- asav_autoscale_params.yaml
- pre_deployment.jinja
- pre_deployment.yaml

Étape 6 Copiez les paquets zip compressés dans le compartiment de stockage.

- `gsutil cp scaleout-action.zip gs://bucket_name`
- `gsutil cp scalein-action.zip gs://bucket_name`

Exemple :

```
pransm@cloudshell:~ (asavgcp-poc-4krn)$ gsutil cp scaleout-action.zip gs://demo-function-bucket
Copying file://scaleout-action.zip [Content-Type=application/zip]...
/ [1 files][  3.3 KiB/  3.3 KiB]
Operation completed over 1 objects/3.3 KiB.
pransm@cloudshell:~ (asavgcp-poc-4krn)$ gsutil cp scalein-action.zip gs://demo-function-bucket
Copying file://scalein-action.zip [Content-Type=application/zip]...
/ [1 files][  3.3 KiB/  3.3 KiB]
Operation completed over 1 objects/3.3 KiB.
pransm@cloudshell:~ (asavgcp-poc-4krn)$
```

Étape 7 Créez un VPC et un sous-réseau pour les interfaces internes, externes et de gestion.

Dans le VPC de gestion, vous devez avoir un sous-réseau/28, par exemple, 10.8.2.0/28.

Étape 8 Vous avez besoin de trois règles de pare-feu pour les interfaces internes, externes et de gestion. En outre, vous devez avoir une règle de pare-feu pour autoriser les sondes de vérification de l'intégrité.

Étape 9 Mettez à jour les paramètres dans les fichiers Jinja et YAML pour le pré-déploiement et le déploiement de l'évolutivité automatique d'ASA virtuel.

a) Ouvrez le fichier `asav_autoscale_params.yaml` et mettez à jour les paramètres suivants :

- **préfixe du nom de la ressource** : <resourceNamePrefix>
- **région** : <region>
- **id de compte de service** : <serviceAccountMailId>
- **Clé publique** : <publicKey>
- **Nom VPC interne** : <Inside-VPC-Name>
- **Sous-réseau VPC interne** : <Inside-VPC-Subnet>
- **Nom VPC externe** :<Outside-VPC-Name>
- **Sous-réseau VPC externe** : <Outside-VPC-Subnet>
- **Nom VPC de gestion** : <Mgmt-VPC-Name>
- **Sous-réseau VPC de gestion** : <Mgmt-VPC-Subnet>
- **Nom de la règle de pare-feu interne** : <Inside-Network-Firewall-Tag>
- **Nom de la règle de pare-feu externe** : <Outside-Network-Firewall-Tag>

- **Nom de la règle de pare-feu de gestion** : <Mgmt-Network-Firewall-Tag>
- **Nom de la règle de pare-feu de vérification de l'intégrité** : <HealthCheck-IP-Firewall-Tag>
- **Type de machine** : <machineType>

Remarque
Pour l'évolutivité automatique d'ASA virtuel, le paramètre **cpuUtilizationTarget: 0.5** est défini et vous pouvez le modifier en fonction de vos besoins.

Cette valeur signifie une utilisation du processeur de 50 % de tout le groupe d'instances ASA virtuel.

b) Ouvrez le fichier `asav_autoscale.jinja` et mettez à jour les paramètres suivants.

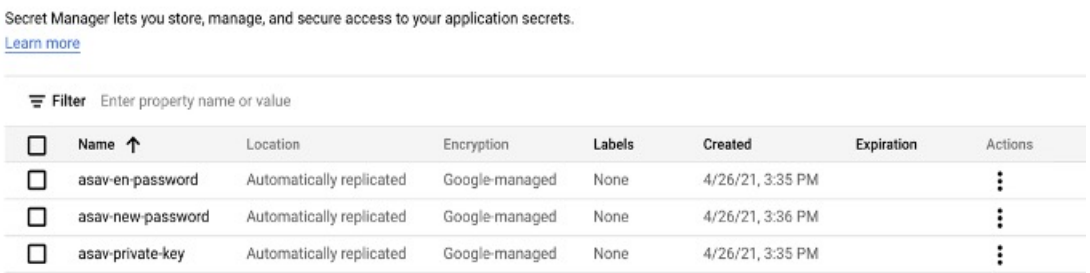
- **hôte** : <Application server IP address>
- **route à l'intérieur de 0.0.0.0 0.0.0.0** : <Inside VPC Gateway IP address> 2
- **gestion de la route 0.0.0.0 0.0.0.0** : <Management VPC Gateway IP address> 3
- **jeton d'ID d'enregistrement des licences smart** : <licenseIDToken>

c) Ouvrez le fichier `pre_deployment.yaml` et mettez à jour les paramètres suivants.

- **préfixe du nom de la ressource** : <resourceNamePrefix>
- **région** : <region>
- **id de compte de service** : <serviceAccountMailId>
- **nom du connecteur VPC** : <VPC-Connector-Name>
- **nom du compartiment** : <bucketName>

Étape 10 Créez trois secrets pour les éléments suivants à l'aide de l'interface graphique utilisateur de Secret Manager. Consultez https://console.cloud.google.com/security/secret-manager.

- asav-en-password
- asav-new-password
- asav-private-key



Étape 11 Créez le connecteur VPC.

```
gcloud beta compute networks vpc-access connectors create <vpc-connector-name>
--region <region> --subnet=</28 subnet name>
```

Exemple :

```
gcloud beta compute networks vpc-access connectors create demo-vpc-connector
--region us-central1 --subnet=outside-connect-28
Create request issued for: [demo-vpc-connector]
Waiting for operation [projects/asavgcp-poc-4krn/locations/us-central1/operations/
10595de7-837f-4c19-9396-0c22943ecf15] to complete...done.
Created connector [demo-vpc-connector].
```

Étape 12 Déployez la configuration YAML de pré-déploiement.

```
gcloud deployment-manager deployments create <pre-deployment-name>
--config pre_deployment.yaml
```

Exemple :

```
gcloud deployment-manager deployments create demo-predeployment
--config pre_deployment.yaml

The fingerprint of the deployment is b'9NOy0gsTPgg16SqUEVsBjA=='
Waiting for create [operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c]...done.
Create operation operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c
completed successfully
```

NOM	TYPE	ÉTAT
demo-asav-delete-sink	gcp-types/logging-v2:projects.sinks	TERMINÉ
demo-asav-insert-sink	gcp-types/logging-v2:projects.sinks	TERMINÉ
demo-asav-pubsub-topic-delete	pubsub.v1.topic	TERMINÉ
demo-asav-pubsub-topic-insert	pubsub.v1.topic	TERMINÉ
demo-asav-scalein-action	gcp-types/cloudfunctions-v1:projects.locations.functions	TERMINÉ
demo-asav-scaleout-action	gcp-types/cloudfunctions-v1:projects.locations.functions	TERMINÉ

Étape 13 Créez le déploiement d'évévolutivité automatique d'ASA virtuel.

```
gcloud deployment-manager deployments create <deployment-name>
--config asav_autoscale_params.yaml
```

Exemple :

```
gcloud deployment-manager deployments create demo-asav-autoscale
--config asav_autoscale_params.yaml
The fingerprint of the deployment is b'1JCQi7Il-laWOY7vOLza0g=='
Waiting for create [operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16]...done.
Create operation operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16
completed successfully.
```

NOM	TYPE	ÉTAT
demo-asav-autoscaler	compute.v1.regionAutoscaler	TERMINÉ
demo-asav-backend-service-elb	compute.v1.regionBackendService	TERMINÉ
demo-asav-backend-service-ilb	compute.v1.regionBackendService	TERMINÉ
demo-asav-fr-elb	compute.v1.forwardingRule	TERMINÉ
demo-asav-fr-ilb	compute.v1.forwardingRule	TERMINÉ
demo-asav-hc-elb	compute.v1.regionHealthChecks	TERMINÉ
demo-asav-hc-ilb	compute.v1.healthCheck	TERMINÉ
demo-asav-health-check	compute.v1.healthCheck	TERMINÉ
demo-asav-instance-group	compute.v1.regionInstanceGroupManager	TERMINÉ
demo-asav-instance-template	compute.v1.instanceTemplate	TERMINÉ
demo-elb-ip	compute.v1.address	TERMINÉ

Étape 14 Créez une route pour qu'ILB transfère les paquets de l'application interne à Internet.

```
gcloud beta compute routes create <ilb-route-name>
--network=<inside-vpc-name> --priority=1000 --destination-range=0.0.0.0/0
--next-hop-ilb=<ilb-forwarding-rule-name> --next-hop-ilb-region=<region>
```

Exemple :

```
gcloud beta compute routes create demo-ilb --network=sdt-test-asav-inside
--priority=1000 --destination-range=0.0.0.0/0 --next-hop-ilb=demo-asav-fr-ilb
--next-hop-ilb-region=us-central1
Created [https://www.googleapis.com/compute/beta/projects/asavgcp-poc-4krn/global
/routes/demo-ilb].
```

NOM	RÉSEAU	PLAGE_DEST	SAUT_SUIVANT	PRIORITÉ
demo-ilb	sdt-test-asav-inside	0.0.0.0/0	10.7.1.60	1000

Étape 15 Créez un routeur et une NAT en nuage.

```
gcloud compute routers create <cloud-router-name>
--project=<project-name> --region <region> --network=<outside-vpc-name>
--advertisement-mode=custom
```

```
gcloud compute routers nats create <cloud-nat-name>
--router=<cloud-router-name> --nat-all-subnet-ip-ranges --auto-allocate-nat-external-ips
--region=<region>
```

Exemple :

```
gcloud compute routers create demo-cloud-router --project=asavgcp-poc-4krn
--region us-central1 --network=sdt-test-asav-outside --advertisement-mode=custom
Creating router [demo-cloud-router]...done.
```

NOM	RÉGION	RÉSEAU
demo-cloud-router	us-central1	sdt-test-asav-outside

```
gcloud compute routers nats create demo-cloud-nat
--router=demo-cloud-router --nat-all-subnet-ip-ranges
--auto-allocate nat-external-ips --region=us-central1
Creating NAT [demo-cloud-nat] in router [demo-cloud-router]...done.
```

Logique d'évolutivité automatique

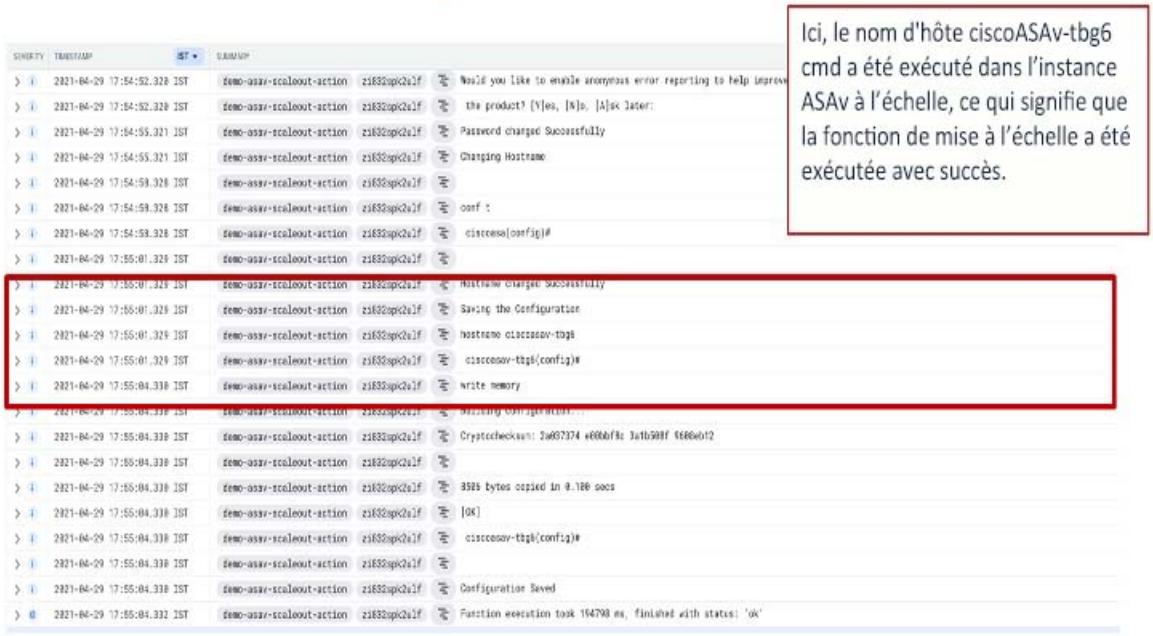
- Le dispositif d'évolutivité automatique traite le niveau d'utilisation du CPU cible comme une fraction de l'utilisation moyenne de tous les vCPU au fil du temps dans le groupe d'instances.
- Si l'utilisation moyenne de vos vCPU totaux dépasse l'utilisation cible, le dispositif d'évolutivité automatique ajoute d'autres instances de VM. Si l'utilisation moyenne de vos vCPU totaux est inférieure à l'utilisation cible, le dispositif d'évolutivité automatique supprime les instances.
- Par exemple, la définition d'une utilisation cible de 0,75 indique au dispositif d'évolutivité automatique de maintenir une utilisation moyenne de 75 % parmi tous les vCPU du groupe d'instances.
- Seules les mesures d'utilisation du CPU sont utilisées dans les décisions en matière d'évolutivité.
- Cette logique est basée sur l'hypothèse que l'équilibreur de charges tentera de répartir également les connexions sur tous les ASA et qu'en moyenne, tous les ASA doivent être chargés de la même manière.

Journalisation et débogage

Les journaux des fonctions en nuage peuvent être consultés comme suit.

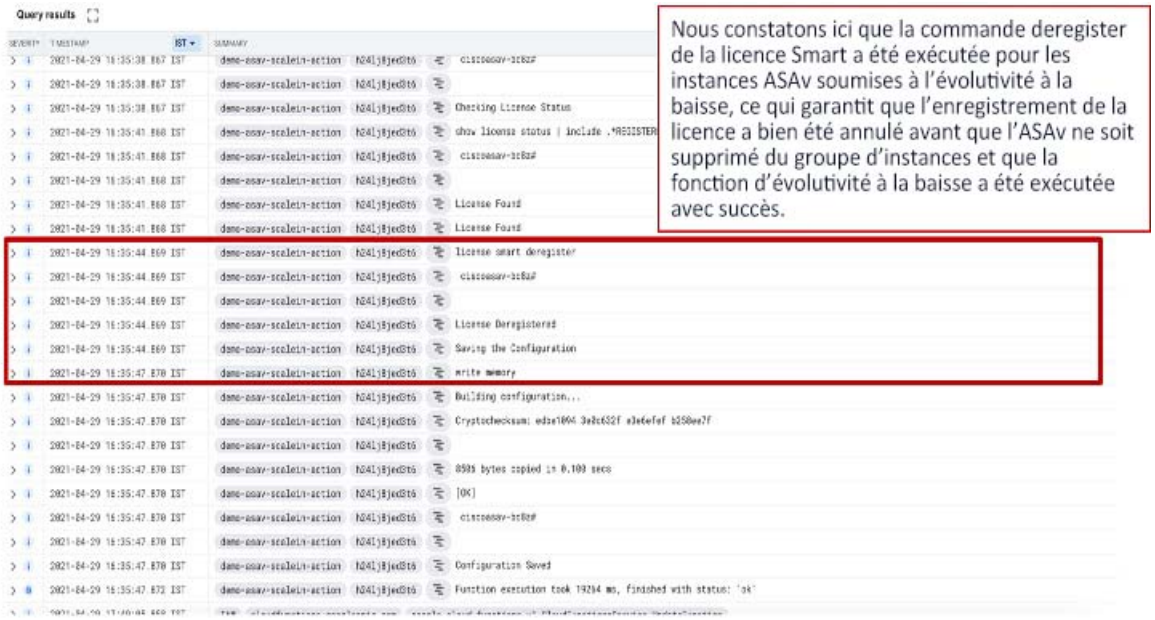
- Journaux de fonction d'évolutivité à la hausse

Illustration 61 : Journaux de fonction d'évolutivité à la hausse



- Journal de fonction d'évolutivité à la baisse

Illustration 62 : Journal de fonction d'évolutivité à la baisse



Lignes directrices et limites relatives à la licence

- Seul IPv4 est pris en charge.
- Les licences prises en charge sont BYOL uniquement. Le protocole PAYG n'est pas disponible pour l'ASA virtuel sur GCP.
- L'équilibreur de charges externe est créé par le modèle et, par conséquent, toute exigence DNS spécifique pour l'adresse IP publique de l'équilibreur de charges est hors du champ d'application.
- Il est supposé que l'application se trouve derrière un équilibreur de charges créé par l'utilisateur et que l'ASA virtuel acheminera tout le trafic vers cet équilibreur de charges (au lieu d'envoyer directement le trafic à une adresse IP d'application spécifique).
- Les détails sur les besoins en matière de configurations de balises, de redondance et d'équilibreur de charges ne sont pas pris en compte.
- Les informations d'authentification d'ASA virtuel vous sont visibles comme suit :
  - Texte en clair dans le code sans serveur.
  - Dans toutes les instances du groupe d'instances.
  - Dans le modèle d'instance, si vous utilisez un compte GCP partagé.

  Ces données sensibles peuvent être protégées à l'aide du service de clé publique de GCP.

Important Cisco recommande de suivre régulièrement l'enregistrement d'ASA virtuel avec le serveur de licences pour vérifier si les ASA soumis à l'évolutivité à la hausse s'enregistrent auprès du serveur de licences comme prévu et si les instances ASA virtuel soumises à l'évolutivité à la baisse sont supprimées du serveur de licences.

Dépannage

Voici des scénarios d'erreurs courants et des conseils de débogage pour l'évolutivité automatique d'ASA virtuel pour GCP :

- `main.py` introuvable : assurez-vous que le paquet zip est créé uniquement à partir des fichiers. Vous pouvez accéder aux fonctions en nuage et vérifier l'arborescence des fichiers. Il ne devrait y avoir aucun dossier.
- Erreur lors du déploiement du modèle : assurez-vous que toutes les valeurs des paramètres dans « <> » sont renseignées dans .jinja et .yaml également, ou que le déploiement du même nom existe déjà.
- La fonction Google ne peut pas atteindre ASA virtuel : assurez-vous que le connecteur VPC est créé et que le même nom est mentionné dans le fichier de paramètres YAML.
- Échec de l'authentification pendant la connexion par SSH ASA virtuel : vérifiez que la paire de clés publique et privée est correcte.
- Échec de l'enregistrement de la licence : assurez-vous que le jeton d'ID de licence est correct. Assurez-vous également que la NAT en nuage est créée et qu'ASA virtuelpeut accéder à tools.cisco.com.

CHAPITRE 14

Déployer l'ASA virtuel sur OpenStack

Vous pouvez déployer l'ASA virtuel sur OpenStack.

- Aperçu, à la page 287
- Préalables pour l'ASA virtuel et OpenStack, à la page 287
- Lignes directrices et limites relatives à la licence, à la page 288
- Configuration système requise, à la page 289
- Exemple de topologie de réseau, à la page 290
- Déployer l'ASA virtuel, à la page 291

Aperçu

Vous pouvez déployer l'ASA virtuel dans un environnement OpenStack. OpenStack est un ensemble d'outils logiciels pour créer et gérer des plateformes d'informatique en nuage pour les clouds publics et privés. Il est parfaitement intégré à l'hyperviseur KVM.

L'activation de la prise en charge de la plateforme OpenStack pour ASA virtuel vous permet d'exécuter ASA virtuel sur des plateformes infonuagiques à code source libre. OpenStack utilise un hyperviseur KVM pour gérer les ressources virtuelles. Les appareils ASA virtuel sont déjà pris en charge sur l'hyperviseur KVM. Par conséquent, il n'y a pas d'ajout supplémentaire de paquets de noyau ou de pilotes pour activer la prise en charge d'OpenStack.

Préalables pour l'ASA virtuel et OpenStack

- Téléchargez le fichier qcow2 ASA virtuel à partir de software.cisco.com et placez-le sur votre hôte Linux :

  http://www.cisco.com/go/asa-software

- L'ASA virtuel prend en charge le déploiement sur l'environnement OpenStack à code source libre et l'environnement OpenStack géré par Cisco VIM.

  Configurez l'environnement OpenStack en fonction des lignes directrices OpenStack.

  - Consultez le document OpenStack à code source libre :

    Version de Wallaby - https://docs.openstack.org/project-deploy-guide/openstack-ansible/wallaby/overview.html

    - Consultez le document OpenStack de Cisco Virtualized Infrastructure Manager (VIM) : Cisco Virtualized Infrastructure Manager Documentation, 4.4.3.

- Obtenez une licence pour l'ASA virtuel. Jusqu'à ce que vous obteniez une licence pour l'ASA virtuel, il fonctionnera en mode dégradé, ce qui n'autorisera que 100 connexions et un débit de 100 kbit/s. Consultez Licences : gestion des licences Smart Software.
- Exigences d'interface :
    - Interface de gestion
    - Interfaces interne et externe
- Chemins de communication :
    - Interface de gestion : utilisée pour connecter l'ASA virtuel à ASDM; ne peut pas être utilisée pour le trafic.
    - Interface interne (requise) : utilisée pour connecter l'ASA virtuel aux hôtes internes.
    - Interface externe (requise) : utilisée pour connecter l'ASA virtuel au réseau public.
- Chemins de communication :
    - Adresses IP flottantes pour l'accès à l'ASA virtuel.
- Version ASA virtuel minimale prise en charge :
    - ASA 9.16.1
- Pour les exigences d'OpenStack, consultez Exigences d'OpenStack.
- Pour les exigences du système ASA virtuel, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

L'ASA virtuel sur OpenStack prend en charge les fonctionnalités suivantes :

- Déploiement d'ASA virtuel sur l'hyperviseur KVM s'exécutant sur un nœud de traitement de votre environnement OpenStack.
- Interface de ligne de commande OpenStack
- Déploiement basé sur un modèle Heat
- Tableau de bord OpenStack Horizon
- Licences : Seul le protocole BYOL est pris en charge
- Gestion d'ASA virtuel à l'aide de l'interface de ligne de commande et ASDM
- Pilotes : VIRTIO et SRIOV

- IPv6

Fonctionnalités non prises en charge

L'ASA virtuel sur OpenStack ne prend pas en charge les éléments suivants :

- Évolutivité automatique
- Grappe

Configuration système requise

L'environnement OpenStack doit être conforme aux exigences matérielles et logicielles prises en charge suivantes.

Tableau 28 : Configuration matérielle et logicielle requise

Type	Versions prises en charge	Notes
Serveur	UCS C240 M5	Il est recommandé de disposer de deux serveurs UCS, un pour le contrôleur OS et un pour le nœud de calcul OS.
Pilote	VIRTIO, IXGBE et I40E	Voici les pilotes pris en charge.
Système d'exploitation	Serveur Ubuntu 20.04	Il s'agit du système d'exploitation recommandé sur les serveurs UCS.
Version OpenStack	Version Wallaby	Des détails sur les différentes versions d'OpenStack sont disponibles à l'adresse suivante : https://releases.openstack.org/

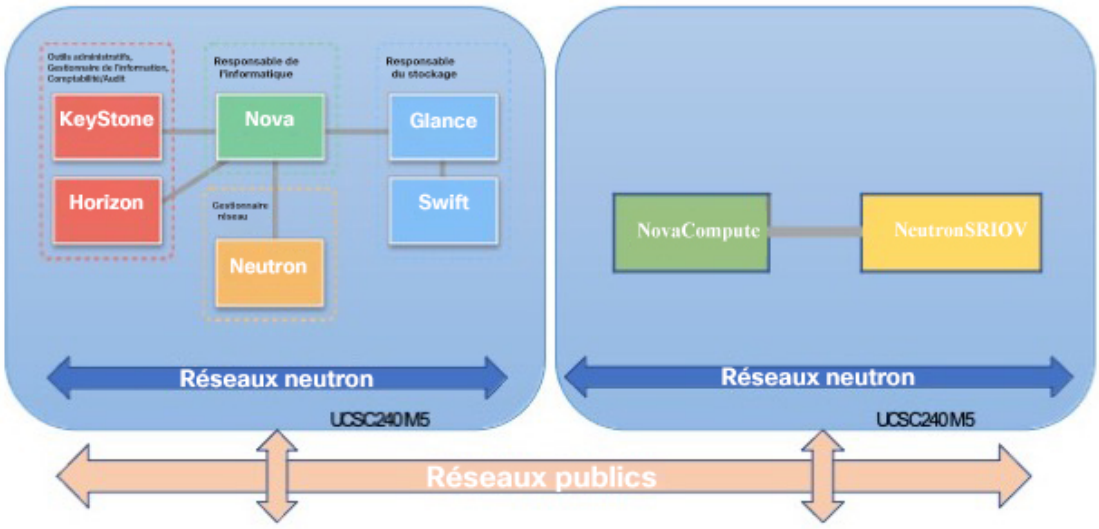
Tableau 29 : Configuration matérielle et logicielle requise pour Cisco VIM Managed OpenStack

Type	Versions prises en charge	Notes
Matériel de serveur	UCS C220-M5/UCS C240-M4	Il est recommandé d'utiliser cinq serveurs UCS, trois pour le contrôleur OS et deux ou plus pour le nœud de calcul du système d'exploitation.
Moteurs	VIRTIO, IXGBE et I40E	Voici les pilotes pris en charge.

Type	Versions prises en charge	Notes
Version de Cisco VIM	Cisco VIM 4.4.3 Pris en charge par : • Système d'exploitation – Red Hat Enterprise Linux 8.4 • Version d'OpenStack – OpenStack 16.2 (version Train)	Reportez-vous à la documentation de Cisco Virtualized Infrastructure Manager, 4.4.3, pour en savoir plus.

Illustration 63 : Topologie de la plateforme OpenStack

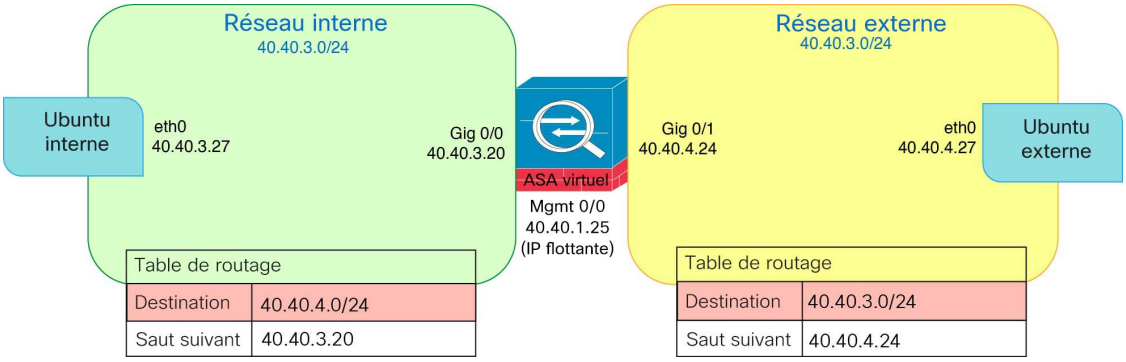
La topologie de la plateforme OpenStack montre la configuration générale d'OpenStack sur deux serveurs UCS.



Exemple de topologie de réseau

La figure suivante montre la topologie de réseau recommandée pour l'ASA virtuel en mode pare-feu routé avec trois sous-réseaux configurés dans OpenStack pour l'ASA virtuel (gestion, interne et externe).

Illustration 64 : Exemple d'ASA virtuel sur le déploiement OpenStack



Déployer l'ASA virtuel

Cisco fournit des exemples de modèles Heat pour le déploiement d'ASA virtuel. Les étapes de création des ressources d'infrastructure OpenStack sont combinées dans un fichier de modèle Heat (`deploy_os_infra.uaml`) pour créer des réseaux, des sous-réseaux et des interfaces de routeur. À un niveau supérieur, les étapes de déploiement de l'ASA virtuel sont classées dans les sections suivantes.

- Chargez l'image ASA virtuel qcow2 vers le service OpenStack Glance.
- Créez l'infrastructure de réseau.
  - Réseau
  - Sous-réseau
  - Interface du routeur
- Créez l'instance ASA virtuel.
  - Saveur
  - Groupes de sécurité
  - IP flottante
  - Instance

Vous pouvez déployer l'ASA virtuel sur OpenStack en utilisant les étapes suivantes.

Charger l'image ASA virtuel dans OpenStack

Copiez l'image qcow2 (`asav-`<version> .qcow2) sur le nœud de contrôleur OpenStack, puis chargez l'image sur le service OpenStack Glance.

Avant de commencer

Téléchargez le fichier qcow2 ASA virtuel à partir de Cisco.com et placez-le sur votre hôte Linux :

http://www.cisco.com/go/asa-software

Remarque Une connexion à Cisco.com et un contrat de service Cisco sont requis.

Procédure

Étape 1 Copiez le fichier image qcow2 sur le nœud de contrôleur OpenStack.

Étape 2 Chargez l'image ASA virtuel sur le service OpenStack Glance.

```
root@ucs-os-controller:$ openstack image create <image_name> --public --disk-
format qcow2 --container-format bare --file ./<asav_qcow2_file>
```

Étape 3 Vérifiez si le chargement de l'image ASA virtuel est réussi.

root@ucs-os-controller:$ openstack image list

Exemple :

```
root@ucs-os-controller:$ openstack image list
+--------------------------------------+----------------------+--------+
| ID                                   | Name                 | Status |+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | asav-<version>-image | active |+
```

L'image chargée et son état sont affichés.

Prochaine étape

Créez l'infrastructure réseau à l'aide du modèle `deploy_os_infra.yaml`.

Créer l'infrastructure réseau pour OpenStack et ASA virtuel

Avant de commencer

Les fichiers de modèle Heat sont nécessaires pour créer l'infrastructure réseau et les composants requis pour ASA virtuel, tels que la convivialité, les réseaux, les sous-réseaux, les interfaces de routeur et les règles de groupe de sécurité :

- `deploy_os_infra.yaml`
- `env.yaml`

Les modèles pour votre version ASA virtuel sont disponibles dans le référentiel GitHub sous Modèle Heat OpenStack ASA virtuel.

Important Notez que les modèles fournis par Cisco sont fournis à titre d'exemples à code source libre et ne sont pas couverts par la portée normale du centre d'assistance technique Cisco. Vérifiez régulièrement GitHub pour connaître les mises à jour et les instructions ReadMe.

Procédure

Étape 1 Déployez le fichier de modèle Heat d'infrastructure.

root@ucs-os-controller:$ opensstack stack create<stack-name> -e<environment files name> -t<deployment file name>

Exemple :

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

Étape 2 Vérifiez si la pile d'infrastructure est créée avec succès.

root@ucs-os-controller:$ openstack stack list

Prochaine étape

Créez l'instance ASA virtuel sur OpenStack.

Créer l'instance ASA virtuel sur OpenStack

Utilisez l'exemple de modèle Heat ASA virtuel pour déployer ASA virtuel sur OpenStack.

Avant de commencer

Un modèle Heat est requis pour déployer l'ASA virtuel sur OpenStack :

- `deploy_asav.yaml`

Les modèles pour votre version ASA virtuel sont disponibles dans le référentiel GitHub sous Modèle Heat OpenStack ASA virtuel.

Important Notez que les modèles fournis par Cisco sont fournis à titre d'exemples à code source libre et ne sont pas couverts par la portée normale du centre d'assistance technique Cisco. Vérifiez régulièrement GitHub pour connaître les mises à jour et les instructions ReadMe.

Procédure

Étape 1 Déployez le fichier de modèle Heat ASA virtuel (`deploy_asav.yaml`) pour créer l'instance ASA virtuel.

root@ucs-os-controller:$ openstack stack create asav-stack -e env.yaml-t deploy_asav.yaml

Exemple :

```
+---------------------+------------------------------+
| Field               | Value                        |
+---------------------+--------------------------------------+
| id                  | 14624af1-e5fa-4096-bd86-c453bc2928ae |
| stack_name          | asav-stack                           |
```

```
| description         | ASAvtemplate                         |
| updated_time        | None                                 |
| stack_status        | CREATE_IN_PROGRESS                   |
| stack_status_reason | Stack CREATE started                 |
+---------------------+--------------------------------------+
```

Étape 2 Vérifiez que votre pile ASA virtuel est créée avec succès.

root@ucs-os-controller:$ openstack stack list

Exemple :

```
+--------------------------------------+-------------+----------------------------------+--------+
| ID                                   | Stack Name  | Project                          | Stack
Status    |
+--------------------------------------+-------------+----------------------------------+----------------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | asav-stack  | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+--------------------------------------+-------------+----------------------------------+----------------+
```

CHAPITRE 15

Déployer l'ASAv sur Nutanix

Ce chapitre décrit la marche à suivre pour déployer l'ASAv dans un environnement Nutanix.

- Aperçu, à la page 295
- Comment déployer l'ASAv sur Nutanix, à la page 299

Aperçu

L'appareil virtuelle de sécurité adaptative Cisco (ASAv) offre des fonctionnalités complètes de pare-feu aux environnements virtualisés afin de sécuriser le trafic des centres de données et les environnements multilocataires.

Vous pouvez déployer l'ASAv sur Nutanix.

Lignes directrices et limites relatives à la licence

Important L'ASAv est déployé avec une taille de stockage sur disque de 8 Go. Il est impossible de modifier l'allocation des ressources de l'espace disque.

Passez en revue les lignes directrices et les limites suivantes avant de déployer l'ASAv.

vNIC recommandées

La vNIC suivante est recommandée pour des performances optimales.

VirtIO : un pilote de réseau para-virtualisé qui prend en charge le fonctionnement à 10 Gbit/s, mais qui nécessite également des cycles du CPU.

Épinglage de CPU

L'épinglage de CPU est nécessaire pour que l'ASAv fonctionne dans un environnement Nutanix; voir Activer l'épinglage du processeur (CPU), à la page 60.

Failover for High Availability

Pour les déploiements de basculement, assurez-vous que l'unité de secours a les mêmes droits de licence; par exemple, les deux unités doivent avoir le droit de 2 Gbit/s.

Important Vous devez ajouter les interfaces de données à chaque ASAv dans le même ordre lors de la création d'une paire à haute accessibilité. Si exactement les mêmes interfaces sont ajoutées à chaque ASAv, mais dans un ordre différent, vous pouvez voir des erreurs sur la console ASAv, ce qui pourrait avoir une incidence sur la fonctionnalité de basculement.

Directives générales

- Le nombre maximal d'interfaces prises en charge est de dix. Vous recevrez un message d'erreur si vous tentez d'ajouter plus de dix interfaces.

Remarque

- Par défaut, l'ASAv configure l'interface de gestion et l'interface interne sur le même sous-réseau.
- Lorsque vous modifiez les interfaces réseau, vous devez désactiver le périphérique ASAv.

- Par défaut, l'ASAv suppose que vous ayez configuré les interfaces de gestion et interne sur les **différents sous-réseaux**. L'interface de gestion a une « IP address DHCP setroute » (Adresse IP DHCP setroute) et la passerelle par défaut est fournie par DHCP.
- L'ASAv doit être sous tension lors du premier démarrage avec au moins trois interfaces. Votre système ne sera pas déployé sans trois interfaces.
- L'ASAv prend en charge un total de 10 interfaces : une interface de gestion (nic0) et un maximum de neuf interfaces réseau (nic1-9) pour le trafic de données. Les interfaces réseau pour le trafic de données peuvent suivre n'importe quel ordre.

Remarque Le nombre minimum d'interfaces réseau pour l'ASAv est de trois interfaces de données.

- Pour l'accès depuis la console, le serveur de terminaux est pris en charge par Telnet.
- Voici les paramètres de mémoire et de vCPU pris en charge :

CPU	Mémoire	Taille de la plateforme ASAv	Type de licence
1	2 Go	1 vCPU/2 Go (par défaut)	1 G (ASAv10)
4	8 Go	4 vCPU/8 Go	2 G (ASAv30)
8	16 Go	8 vCPU/16 Go	10 G (ASAv50)
16	32 Go	16 vCPU/32 Go	20 G (ASAv100)

Fonctionnalités prises en charge

- Mode routé (par défaut)
- Mode transparent

Remarque La chaîne de services dans une grappe multi-nœuds n'est pas prise en charge en mode transparent.

Consultez la concordance suivante concernant les adaptateurs réseau, les réseaux sources et les réseaux de destination pour les interfaces ASAv :

Adaptateur réseau	Réseau source	Réseaux de destination	Fonction
vnic0	Management0-0	Management0/0	Gestion
vnic1	GigabitEthernet0-1	GigabitEthernet 0/1	Partie
vnic2	GigabitEthernet0-2	GigabitEthernet 0/2	Intérieur
vnic3-9	Données	Données	Données

ASAv sur Proxmox VE

Proxmox Virtual Environment (VE) est une plateforme de virtualisation de serveurs à code source libre qui peut gérer les machines virtuelles Nutanix. Proxmox VE fournit également une interface de gestion web.

Lorsque vous déployez l'ASAv sur Proxmox VE, vous devez configurer la VM pour qu'elle ait un port série émulé. Sans le port série, l'ASAv entrera en boucle pendant le processus de démarrage. Toutes les tâches de gestion peuvent être effectuées à l'aide de l'interface de gestion web Proxmox VE.

Remarque Pour les utilisateurs avancés qui sont habitués au confort de l'interface Shell Unix ou de Windows Powershell, Proxmox VE fournit une interface de ligne de commande pour gérer tous les composants de votre environnement virtuel. Cette interface de ligne de commande dispose d'une fonction intelligente de complétion par tabulation et d'une documentation complète sous forme de pages de manuel UNIX.

Pour que l'ASAv démarre correctement, la VM doit avoir un périphérique série configuré :

1. Dans le centre de gestion principal, sélectionnez la VM ASAv dans l'arborescence de navigation de gauche.
2. Mettez la machine virtuelle hors tension.
3. Choisissez **Hardware (Matériel)** > **Add (Ajouter)** > **Network Device (Appareil réseau)** et ajoutez un port série.
4. Mettez l'ordinateur virtuel sous tension.
5. Accédez à la VM ASAv à l'aide de Xterm.js.

Consultez la page Terminal série de Proxmox pour en savoir plus sur la configuration et l'activation du terminal sur l'invité ou le serveur.

Fonctionnalités non prises en charge

- L'ASAv sur Nutanix AHV ne prend pas en charge l'enfichage à chaud de l'interface. N'essayez pas d'ajouter ou de supprimer des interfaces lorsque l'ASAv est sous tension.
- Nutanix AHV ne prend pas en charge la virtualisation des E/S à racine unique (SR-IOV) ou l'ensemble de développement de plan de données Open vSwitch (DPDK-OVS).

Remarque Nutanix AHV prend en charge DPDK sur invité à l'aide de VirtIO. Pour en savoir plus, consultez Prise en charge de DPDK sur AHV.

Documentation associée

- Notes de version Nutanix
- Guide d'installation de terrain Nutanix
- Support matériel sur Nutanix
- Prise en charge multifile d'attente pour Virtio-Net sur Nutanix AHV

Configuration système requise

Version d'ASA

9.16.2

Mémoire ASAv, vCPU et taille de disque

Le matériel spécifique utilisé pour les déploiements d'ASAv peut varier en fonction du nombre d'instances déployées et des exigences d'utilisation. Chaque instance d'ASAv nécessite une allocation minimale de ressources (quantité de mémoire, nombre de CPU et espace disque) sur le serveur.

Licences ASAv

- Configurez tous les droits de licence pour les services de sécurité à partir de l'interface de ligne de commande d'ASAv.
- Consultez *ASAv : Configurer les licences logicielles Smart* dans le Guide de configuration Cisco ASA pour en savoir plus sur la gestion des licences.

Composants et versions de Nutanix

Composant	Version
Système d'exploitation Nutanix Acropolis (AOS)	5.15.5 LTS ou version ultérieure

Composant	Version
Nutanix Cluster Check (NCC)	4.0.0.1
Nutanix AHV	20201105.12 et version ultérieure

Comment déployer l'ASAv sur Nutanix

Étape	Tâche	Autres renseignements
1	Passez en revue les conditions préalables.	Prérequis, à la page 299
2	Chargez le fichier ASAv qcow2 dans l'environnement Nutanix.	Charger le fichier QCOW2 dans Nutanix, à la page 299
3	Préparez un fichier de configuration Day 0 (jour 0) avec les données de configuration initiale qui sont appliquées au moment du déploiement d'une machine virtuelle.	Préparer le fichier de configuration Day0 (Jour0), à la page 300
4	Déployez l'ASAv sur Nutanix.	Déployer l'ASA virtuel, à la page 302
5	Lancer l'ASAv.	Lancer l'ASA virtuel , à la page 304

Prérequis

- Téléchargez le fichier qcow2 ASAv à partir de Cisco.com et placez-le sur votre hôte Linux :

  http://www.cisco.com/go/asa-software

Remarque Une connexion à Cisco.com et un contrat de service Cisco sont requis.

- Pour la compatibilité du logiciel ASA et de l'ASAv HyperFlex, consultez la section Compatibilité Cisco ASA.

Charger le fichier QCOW2 dans Nutanix

Pour déployer l'ASAv dans l'environnement Nutanix, vous devez créer une image à partir du fichier disque qcow2 dans la console Web Prism.

Avant de commencer

Téléchargez le fichier disque qcow2 à partir de Cisco.com : https://software.cisco.com/download/navigator.html

Procédure

Étape 1 Connectez-vous à la console Web Nutanix Prism.

Étape 2 Cliquez sur l'icône en forme d'engrenage pour ouvrir la page **Settings** (paramètres).

Étape 3 Cliquez sur **Image Configuration** (configuration de l'image) dans le volet gauche.

Étape 4 Cliquez sur **Upload Image** (charger une image).

Étape 5 Créez l'image.

1. Saisissez un nom pour l'image.
2. Dans la liste déroulante **Image Type** (type d'image), sélectionnez **DISK** (disque).
3. Dans la liste déroulante **Storage Container** (conteneur de stockage), choisissez le conteneur souhaité.
4. Précisez l'emplacement du fichier disque qcow2.

   Vous pouvez soit préciser une URL (pour importer le fichier à partir d'un serveur Web), soit charger le fichier à partir de votre ordinateur.
5. Cliquez sur **Save** (enregistrer).

Étape 6 Attendez que la nouvelle image s'affiche dans la page **Image Configuration** (configuration d'image).

Préparer le fichier de configuration Day0 (Jour0)

Vous pouvez préparer un fichier de configuration Day0 (Jour0) avant de déployer l'ASAv. Ce fichier est un fichier texte qui contient les données de configuration initiale qui sont appliquées lors du déploiement d'une machine virtuelle.

Si vous effectuez le déploiement avec un fichier de configuration Day0 (Jour0), le processus vous permet d'effectuer la configuration initiale complète de l'appareil ASAv.

Dans le fichier, vous pouvez spécifier les éléments suivants :

- Un nom de domaine pour le système.
- Un nouveau nom d'utilisateur et un nouveau mot de passe d'administrateur pour le compte admin.
- Le mode de pare-feu initial; définit le mode de pare-feu initial, **routed** (routé) ou **transparent**.

  Si vous prévoyez de gérer votre déploiement à l'aide du réseau local, vous ne pouvez saisir que **routed** (routé) pour le mode de pare-feu. Vous ne pouvez pas configurer des interfaces en mode de pare-feu transparent à l'aide du gestionnaire d'appareil ASAv.

- ASDM à activer :
  - **activation du serveur http**
  - **accès mondial à tous les groupes**
  - **gestion de http 0.0.0.0 0.0.0.0**

- Liste d'accès
- Serveur de noms
- Paramètres réseau qui permettent à l'appareil de communiquer sur votre réseau de gestion.

Remarque Vous pouvez soit charger le fichier de configuration Day0 (Jour0), soit copier et coller le contenu dans la zone de texte fournie.

Procédure

Étape 1 Créez un nouveau fichier texte à l'aide d'un éditeur de texte de votre choix.

Étape 2 Saisissez les détails de la configuration dans le fichier texte, comme illustré dans l'exemple suivant :

Exemple :

```
ASA Version 9.16.2
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
```

La première ligne doit commencer par la version de l'ASA. La configuration day0-config doit être une configuration ASA valide. La meilleure façon de générer la configuration day0 (jour0) est de copier les parties pertinentes d'une configuration en cours d'exécution à partir d'un ASA ou d'un ASAv existant. L'ordre des lignes dans la configuration day0 (jour0) est important et doit correspondre à l'ordre observé dans une sortie de commande **show running-config** existante.

Configuration day0 (jour0) possible

- Nom d'hôte
- Nom de domaine
- Mot de passe administratif

- Interfaces
- Adresses IP
- du routage statique;
- Serveur DHCP
- Règles de traduction des adresses réseau

Remarque
Le contenu du fichier de configuration Day0 (Jour0) doit être au format JSON. Vous devez valider le texte à l'aide d'un outil de validation JSON.

Étape 3 Enregistrez le fichier sous le nom `day0-config.txt`.

Étape 4 Sélectionnez l'option **Custom Script** (Personnaliser le script).

Étape 5 Vous pouvez soit charger le fichier `day0-config.txt`, soit copier et coller le fichier dans la zone de texte fournie.

Étape 6 Répétez les étapes 1 à 3 pour créer des fichiers de configuration par défaut uniques pour chaque ASAv que vous souhaitez déployer.

Déployer l'ASA virtuel

Avant de commencer

Assurez-vous que l'image de l'ASAv que vous prévoyez de déployer apparaît sur la page **Image Configuration** (Configuration de l'image).

Procédure

Étape 1 Connectez-vous à la console Web Nutanix Prism.

Étape 2 Dans la barre de menu principale, cliquez sur la liste déroulante **View** (Afficher) et sélectionnez **VM**.

Étape 3 Dans le tableau de bord de la VM, cliquez sur **Create VM** (Créer une VM).

Étape 4 Procédez comme suit :

1. Saisissez un nom pour l'instance ASAv.
2. (Facultatif) Saisissez une description pour l'instance ASAv.
3. Sélectionnez le fuseau horaire que vous souhaitez que l'instance ASAv utilise.

Étape 5 Entrez les détails du calcul.

1. Saisissez le nombre de CPU virtuels à allouer à l'instance ASAv.
2. Saisissez le nombre de cœurs qui doivent être affectés à chaque CPU virtuel.
3. Saisissez la quantité de mémoire (en Go) à allouer à l'instance ASAv.

Étape 6 Associez un disque à l'instance ASAv.

1. Sous **Disks** (Disques), cliquez sur **Add New Disk** (Ajouter un nouveau disque).
2. Dans la liste déroulante **Type**, choisissez **DISK** (DISQUE).
3. Dans la liste déroulante **Operation** (Opération), choisissez **Clone from Image Service** (Cloner à partir du service d'image).
4. Dans la liste déroulante **Bus Type** (Type de bus), choisissez **DISK** (DISQUE).
5. Dans la liste déroulante **Image**, choisissez l'image que vous souhaitez utiliser.
6. Cliquez sur **Add** (Ajouter).

Étape 7 Configurez au moins trois interfaces de réseau virtuel.

Sous **Network Adapters (NIC)** (Adapateurs réseau (NIC)), cliquez sur **Add New NIC** (Ajouter une nouvelle carte réseau), sélectionnez un réseau et cliquez sur **Add** (Ajouter).

Répétez ce processus pour ajouter d'autres interfaces réseau.

L'ASAv sur Nutanix prend en charge un total de dix interfaces : une interface de gestion et un maximum de neuf interfaces réseau pour le trafic de données. Les affectations interface-réseau doivent être ordonnées comme suit :

- vnic0 : interface de gestion (obligatoire)
- vnic1 : interface externe (obligatoire)
- vnic2 : interface interne (obligatoire)
- vnic3-9 : interface de données (facultatif)

Étape 8 Configurez la politique d'affinité pour l'ASAv.

Sous **VM Host Affinity** (Affinité d'hôte VM), cliquez sur **Set Affinity** (Définir l'affinité), sélectionnez les hôtes et cliquez sur **Save** (Enregistrer).

Sélectionnez plusieurs hôtes pour vous assurer que la VM peut s'exécuter même en cas de défaillance de nœud.

Étape 9 Si vous avez préparé un fichier de configuration Day0 (Jour0), procédez comme suit :

1. Sélectionnez **Custom Script** (Script personnalisé).
2. Cliquez sur **Upload A File** (Charger un fichier) et sélectionnez le fichier de configuration Day0 (Jour0) `day0-config.txt` ou copiez et collez le contenu dans une zone de texte.

Remarque
Toutes les autres options de scripts personnalisés ne sont pas prises en charge dans la version.

Étape 10 Cliquez sur **Save** (Enregistrer) pour déployer l'instance ASAv. L'instance apparaît dans la vue du tableau de la VM.

Étape 11 Dans la vue du tableau la VM, sélectionnez l'instance nouvellement créée, et cliquez sur **Power On** (Démarrer).

Lancer l'ASA virtuel

Une fois que la machine virtuelle est sous tension, sélectionnez **ASAv-VM** > **Launch Console** (lancer la console) avec le nom d'utilisateur et le mot de passe prédéfinis en y accédant par le biais du fichier `day0-config`.

Remarque Pour modifier l'un de ces paramètres d'un appareil virtuel après avoir terminé la configuration initiale, vous devez utiliser l'interface de ligne de commande.

Procédure

Étape 1 Cliquez sur **Launch Console** (lancer la console) pour accéder à l'ASAv déployé.

Étape 2 À l'invite **asav login** (connexion d'asav), connectez-vous avec le **nom d'utilisateur** et le **mot de passe** de `day0-config`.

CHAPITRE 16

Déployer l'ASAv sur Cisco HyperFlex

Les systèmes HyperFlex offrent une hyperconvergence pour toutes les applications et partout. Hyperflex, associé à la technologie Cisco Unified Computing System (Cisco UCS) gérée par la plateforme d'exploitation du nuage Cisco Intersight, peut propulser les applications et les données n'importe où, optimiser les opérations d'un centre de données central vers la périphérie et dans les nuages publics, et augmenter ainsi l'agilité en accélérant les pratiques DevOps.

Ce chapitre décrit le fonctionnement de l'ASAv dans un environnement Cisco HyperFlex, y compris la prise en charge des fonctionnalités, les exigences du système, les lignes directrices et les limites.

Important La mémoire minimale requise pour l'ASAv est de 2 Go. Si votre ASAv actuel fonctionne avec moins de 2 Go de mémoire, vous ne pouvez pas effectuer de mise à niveau vers la version 9.13(1)+ à partir d'une version antérieure sans augmenter la mémoire de votre VM ASAv. Vous pouvez également redéployer une nouvelle VM ASAv avec la dernière version.

- Lignes directrices et limites relatives à la licence, à la page 305
- Déployer l'ASA virtuel, à la page 309
- Mettre à niveau la licence vCPU ou de débit, à la page 316
- Réglage de la performance, à la page 317

Lignes directrices et limites relatives à la licence

Vous pouvez créer et déployer plusieurs instances d'ASAv Cisco HyperFlex sur un serveur VMware vCenter. Le matériel spécifique utilisé pour les déploiements d'ASAv peut varier en fonction du nombre d'instances déployées et des exigences d'utilisation. Chaque appliance virtuelle que vous créez nécessite une allocation minimale de ressources (mémoire, nombre de CPU et espace disque) sur la machine hôte.

Important L'ASAv est déployé avec une taille de stockage sur disque de 8 Go. Il est impossible de modifier l'allocation des ressources de l'espace disque.

Passez en revue les lignes directrices et les limites suivantes avant de déployer l'ASAv.

vNIC recommandées

Pour des performances optimales, nous vous recommandons d'utiliser le vNIC vmxnet3. Ce vNIC est un pilote de réseau para-virtualisé qui prend en charge le fonctionnement à 10 Gbit/s, mais nécessite également des cycles du CPU. De plus, lorsque vous utilisez vmxnet3, désactivez le Large Receive Offload (LRO, déchargement important à la réception) pour éviter de mauvaises performances TCP.

Lignes directrices relatives aux fichiers OVF

- asav-vi.ovf – Pour le déploiement sur vCenter
- Le déploiement OVF d'ASAv ne prend pas en charge la localisation (installation des composants en mode non anglais). Assurez-vous que VMware vCenter et les serveurs LDAP de votre environnement sont installés dans un mode compatible avec ASCII.
- Vous devez régler votre clavier à l'anglais des États-Unis avant d'installer l'ASAv et pour utiliser la console de VM.

Lignes directrices relatives au basculement pour la haute disponibilité

Pour les déploiements de basculement, assurez-vous que l'unité de secours a les mêmes droits de licence; par exemple, les deux unités doivent avoir le droit de 2 Gbit/s.

Important Lors de la création d'une paire à haute accessibilité à l'aide d'ASAv, vous devez ajouter les interfaces de données à chaque ASAv dans le même ordre. Si vous avez ajouté exactement les mêmes interfaces à chaque ASAv, mais dans un ordre différent, vous pourriez voir des erreurs sur la console ASAv. La fonctionnalité de basculement peut également être affectée.

Directives IPv6

Vous ne pouvez pas préciser d'adresses IPv6 pour l'interface de gestion lorsque vous déployez le fichier OVF ASAv pour la première fois à l'aide du client web VMware vSphere; vous pourrez ajouter ultérieurement l'adressage IPv6 à l'aide d'ASDM ou de l'interface de ligne de commande.

Lignes directrices vMotion

- VMware vous demande de n'utiliser que le stockage partagé si vous utilisez vMotion. Pendant le déploiement d'ASAv, si vous avez une grappe d'hôtes, vous pouvez provisionner le stockage localement (sur un hôte précis) ou sur un hôte partagé. Cependant, si vous essayez d'utiliser l'ASAV vMotion vers un autre hôte, l'utilisation du stockage local produira une erreur.

Allocation de mémoire et de vCPU pour le débit et les licences

- La mémoire allouée à l'ASAv est d'une taille spécifique pour le niveau de débit. Ne modifiez pas les paramètres de mémoire ni les paramètres matériels de vCPU dans la boîte de dialogue **Edit Settings** (Modifier les paramètres), sauf si vous demandez une licence pour un autre niveau de débit. Le provisionnement insuffisant peut affecter les performances.

Remarque Si vous devez modifier la mémoire ou les paramètres matériels vCPU, utilisez uniquement les valeurs documentées dans Gestion des licences pour l'ASA virtuel, à la page 1. N'utilisez pas les valeurs minimales, par défaut et maximales de configuration de mémoire recommandées par VMware.

Réservation de CPU

- Par défaut, la réservation de CPU pour l'ASAv est de 1 000 MHz. Vous pouvez modifier la quantité de ressources de CPU allouées à l'ASAv en utilisant les paramètres de partages, de réservations et de limites. **Edit Settings (Modifier les paramètres)** > **Resources (Ressources)** > **CPU**. L'abaissement du paramètre de réservation de CPU de 1 000 MHz peut être effectué si l'ASAv peut réaliser l'objectif requis tout en étant sous la charge de trafic requise avec le paramètre inférieur. La quantité de CPU utilisée par un ASAv dépend de la plateforme matérielle sur laquelle il s'exécute, ainsi que du type et de la quantité de travail qu'il effectue.

  Vous pouvez afficher le point de vue de l'hôte sur l'utilisation du CPU pour toutes vos machines virtuelles à partir du tableau d'utilisation du CPU (MHz), situé dans la vue Home (Accueil) de l'onglet Virtual Machine Performance (Performances de la machine virtuelle). Une fois que vous avez établi un test de référence pour l'utilisation du CPU lorsque l'ASAv traite le volume de trafic typique, vous pouvez utiliser ces renseignements comme entrée pour ajuster la réservation du CPU.

  Pour en savoir plus, consultez le lien Conseil d'amélioration des performances du CPU
- Vous pouvez afficher l'allocation des ressources et toutes les ressources qui sont surprovisionnées ou sous-provisionnées à l'aide des commandes**show vm** > **show cpu**de l'ASAv,

  de l'onglet

  Home (Accueil) > **Device Dashboard (Tableau de bord des appareils)** > **Device Information (Renseignements sur l'appareil)** > **Virtual Resources (Ressources virtuelles)**

  ou du volet

  Monitoring (Supervision) > **Properties (Propriétés)** > **System Resources Graphs (Graphiques des ressources du système)** > **CPU**.

Lignes directrices relatives au mode transparent sur le matériel UCS de série B et C

Des intermittences MAC ont été observées dans certaines configurations d'ASAv fonctionnant en mode transparent sur le matériel Cisco UCS de série B (nœuds de traitement informatique) et C (nœuds convergés). Lorsque des adresses MAC apparaissent à partir de différents emplacements, vous obtiendrez des paquets abandonnés.

Les lignes directrices suivantes aident à éviter les intermittences MAC lorsque vous déployez l'ASAv en mode transparent dans les environnements VMware :

- Regroupement NIC VMware : si vous déployez l'ASAv en mode transparent sur le matériel UCS de série B ou C, les groupes de ports utilisés pour les interfaces interne et externe ne doivent avoir qu'un seul lien ascendant actif, qui doit être le même. Configurez le regroupement de NIC VMware dans vCenter.
- Inspection ARP : activez l'inspection ARP sur l'ASAv et configurez de manière statique les entrées MAC et ARP sur l'interface sur laquelle vous souhaitez les recevoir. Consultez le Guide de configuration

des opérations générales de la série Cisco ASA pour en savoir plus sur l'inspection ARP et sur la façon de l'activer.

Configuration système requise

Configurations et grappes pour les systèmes Hyperflex de série HX

Configurations	Grappes
Nœuds convergés HX220c	• Grappe de flash • Au moins une grappe de 3 nœuds (bases de données, VDI, VSI)
Nœuds convergés HX240c	• Grappe de flash • Au moins une grappe de 3 nœuds (VSI : applications informatiques/affaires, test/développement)
HX220C et Edge (VDI, VSI, ROBO) HX240C (VDI, VSI, test/développement)	• Grappe hybride • Au moins une grappe de 3 nœuds
B200 + C240/C220	Applications liées à l'informatique/VDI

Options de déploiement pour le périphérique Hyperflex de série HX :

- Grappe hybride
- Grappe flash
- HyperFlex Edge
- Lecteurs SED
- Cache NVME
- GPU

Pour l'option de gestion en nuage HyperFlex HX, consultez la section sur le *déploiement des grappes reliées à l'interconnexion* de la trame HyperFlex dans le Guide d'installation de Cisco HyperFlex Systems.

Composants et versions d'HyperFlex

Composant	Version
VMware vSphere	7.0.2-18426014
Plateforme de données HyperFlex	4.5.2a-39429

Fonctionnalités prises en charge

- Modes de déploiement : routage (autonome), routage (HA) et transparent
- ASAv haute disponibilité en natif
- Bâtis grand format
- virtio
- Grappes de centre de données Hyperflex (à l'exception des grappes étendues)
- Grappes de HyperFlex Edge
- Nœuds convergés HyperFlex All NVMe, All Flash et Hybrid
- Nœuds de traitement informatique Hyperflex uniquement

Fonctionnalités non prises en charge

ASAv exécuté avec SR-IOV n'a pas été qualifié avec HyperFlex.

Remarque HyperFlex prend en charge SR-IOV, mais nécessite une carte réseau PCI-e en plus du VIC MLOM

Déployer l'ASA virtuel

Étape	Tâche	Autres renseignements
1	Examinez les lignes directrices et les limites.	Lignes directrices et limites relatives à la licence, à la page 305
2	Passez en revue les conditions préalables.	Conditions préalables pour l'ASAv et Cisco HyperFlex, à la page 309
3	Téléchargez le fichier OVF à partir de cisco.com.	Télécharger et décompresser le logiciel ASAv, à la page 310
4	Déployez l'ASAv sur Cisco HyperFlex.	Déployer l'ASAv sur Cisco HyperFlex dans vSphere vCenter, à la page 311
5	Accédez à la console ASAv.	Accéder à la console ASAv, à la page 313

Conditions préalables pour l'ASAv et Cisco HyperFlex

Vous pouvez déployer l'ASAv sur Cisco HyperFlex à l'aide du client web VMware vSphere, du client autonome vSphere ou de l'outil OVF. Consultez la section Compatibilité Cisco ASA pour connaître les exigences du système.

Politique de sécurité pour un commutateur standard vSphere

Pour un commutateur vSphere, vous pouvez modifier les politiques de sécurité de couche 2 et appliquer des exceptions aux politiques de sécurité pour les groupes de ports utilisés par les interfaces ASAv. Consultez les paramètres par défaut suivants :

- Mode promiscuité : **Reject** (Refuser)
- Modifications d'adresses MAC : **Accept** (Accepter)
- Transmissions forgées : **Accept** (Accepter)

Vous devrez peut-être modifier ces paramètres pour les configurations ASAv suivantes. Consultez la documentation de vSphere pour en savoir plus.

Tableau 30 : Exceptions à la politique de sécurité du groupe de ports

Exception de sécurité	Mode de pare-feu routé		Mode de pare-feu transparent	
	Aucun basculement	Basculement	Aucun basculement	Basculement
Mode Promiscuous	<any>	<any>	Accepter	Accepter
Modifications d'adresses MAC :	<any>	Accepter	<any>	Accepter
Transmissions forgées	<any>	Accepter	Accepter	Accepter

Télécharger et décompresser le logiciel ASAv

Avant de commencer

Vous devez avoir au moins un réseau configuré dans vSphere (pour la gestion) avant de déployer l'ASAv.

Procédure

Étape 1 Téléchargez le fichier ZIP à partir de Cisco.com et enregistrez-le sur votre disque local :

https://www.cisco.com/go/asa-software

Remarque
Une connexion à Cisco.com et un contrat de service Cisco sont requis.

Étape 2 Décompressez le fichier dans un répertoire de travail. Ne supprimez aucun fichier du répertoire. Les fichiers suivants sont inclus :

- asav-vi.ovf : pour les déploiements vCenter.
- boot.vmdk – Démarrer l'image du disque.
- disk0.vmdk : image disque pour l'ASAv.
- day0.iso : ISO contenant un fichier day0-config et éventuellement un fichier idtoken.

• asav-vi.mf : fichier manifeste pour les déploiements vCenter.

Déployer l'ASAv sur Cisco HyperFlex dans vSphere vCenter

Utilisez cette procédure pour déployer l'ASAv sur HyperFlex sur VMware vSphere vCenter. Vous pouvez utiliser le client web VMware (ou le client vSphere) pour déployer et configurer des machines virtuelles.

Avant de commencer

Vous devez avoir au moins un réseau configuré dans vSphere (pour la gestion) avant de déployer l'ASAv sur HyperFlex.

Avant d'installer l'ASAv sur la grappe HyperFlex, la grappe HyperFlex et le magasin de données partagé doivent être créés. Consultez le guide de configuration HyperFlex pour en savoir plus.

Procédure

Étape 1 Connectez-vous au client web vSphere.

Étape 2 À l'aide du client web vSphere, déployez le fichier de modèle OVF que vous avez téléchargé précédemment en cliquant sur **ACTIONS** > **Deploy OVF Template** (Déployer le modèle OVF).

L'assistant de déploiement du modèle OVF s'affiche.

Étape 3 Parcourez votre système de fichiers pour trouver l'emplacement source du modèle OVF, puis cliquez sur **NEXT** (SUIVANT).

Étape 4 Passez en revue la page **OVF Template Details** (Détails du modèle OVF) et vérifiez les renseignements sur le modèle OVF (nom du produit, version, prestataire, taille de téléchargement, taille sur le disque et description), puis cliquez sur **NEXT** (SUIVANT).

Étape 5 La page **End User License Agreement** (Contrat de licence de l'utilisateur final) s'affiche. Passez en revue le contrat de licence groupé avec le modèle OVF (modèles VI uniquement), cliquez sur **Accept** (Accepter) pour accepter les conditions des licences et cliquez sur **NEXT** (SUIVANT).

Étape 6 Sur la page **Name and Location** (Nom et emplacement), saisissez un nom pour ce déploiement et sélectionnez un emplacement dans l'inventaire (magasin de données partagé ou grappe) sur lequel vous souhaitez déployer HyperFlex, puis cliquez sur **NEXT** (SUIVANT). Le nom doit être unique dans le dossier d'inventaire et peut contenir jusqu'à 80 caractères.

Le client web vSphere présente la hiérarchie organisationnelle des objets gérés dans des vues d'inventaire. Les inventaires sont la structure hiérarchique utilisée par le serveur vCenter ou l'hôte pour organiser les objets gérés. Cette hiérarchie inclut tous les objets surveillés dans le serveur vCenter.

Étape 7 Accédez à et sélectionnez l'ensemble de ressources dans lequel vous souhaitez exécuter l'ASAv HyperFlex, puis cliquez sur **NEXT** (SUIVANT).

Remarque
Cette page s'affiche uniquement si la grappe contient un ensemble de ressources. Pour l'ensemble de ressources de calcul, nous recommandons uniquement la grappe pour obtenir les meilleures performances.

Étape 8 Sélectionnez une **Deployment Configuration** (Configuration de déploiement). Choisissez l'une des trois valeurs de vCPU/mémoire prises en charge dans la liste déroulante **Configuration**, puis cliquez sur **NEXT** (SUIVANT).

Étape 9 Sélectionnez un emplacement de **Storage** (Stockage) pour stocker les fichiers de la machine virtuelle, puis cliquez sur **NEXT** (SUIVANT).

Sur cette page, sélectionnez les magasins de données (le magasin de données est un magasin de données partagé de grappe HX créé avec HX connect) qui est déjà configuré sur la grappe de destination. Le fichier de configuration de la machine virtuelle et les fichiers de disque virtuel sont stockés dans le magasin de données. Sélectionnez un magasin de données suffisamment grand pour contenir la machine virtuelle et tous ses fichiers de disque virtuel.

Étape 10 Sur la page **Network Mapping** (Mappage du réseau), mappez les réseaux spécifiés dans le modèle OVF aux réseaux de votre inventaire, puis sélectionnez **NEXT** (SUIVANT).

Assurez-vous que l'interface Management0-0 est associée à un réseau de VM accessible à partir d'Internet. Les interfaces qui ne sont pas des interfaces de gestion sont configurables à partir d'un centre de gestion ASAv ou d'un gestionnaire d'appareil ASAv, selon votre mode de gestion.

Important
ASAv sur HyperFlex utilise maintenant les interfaces vmxnet3 par défaut lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Si vous utilisez des interfaces e1000, nous vous **recommandons fortement** de changer. Les pilotes de périphérique vmxnet3 et le traitement réseau sont intégrés à HyperFlex. Ils utilisent donc moins de ressources et offrent de meilleures performances réseau.

Les réseaux ne peuvent pas être en ordre alphabétique. S'il est trop difficile de trouver vos réseaux, vous pouvez modifier les réseaux plus tard à partir de la boîte de dialogue **Edit Settings** (Modifier les paramètres). Après le déploiement, cliquez avec le bouton droit sur l'instance et choisissez **Edit Settings** (Modifier les paramètres). Cependant, la page de mappage du réseau n'affiche pas les ID (uniquement les ID d'adaptateur réseau).

Consultez la concordance suivante concernant l'adaptateur réseau, les réseaux sources et les réseaux de destination pour les interfaces (il s'agit des interfaces vmxnet3 par défaut) :

Tableau 31 : Mappage du réseau source au réseau de destination : VMXNET3

ID d'adaptateur réseau	ID d'interface ASAv
Adaptateur réseau 1	Management 0/0
Adaptateur réseau 2	GigabitEthernet 0/0
Adaptateur réseau 3	GigabitEthernet 0/1
Adaptateur réseau 4	GigabitEthernet 0/2
Adaptateur réseau 5	GigabitEthernet 0/3
Adaptateur réseau 6	GigabitEthernet 0/4
Adaptateur réseau 7	GigabitEthernet 0/5
Adaptateur réseau 8	GigabitEthernet 0/6
Adaptateur réseau 9	GigabitEthernet 0/7
Adaptateur réseau 10	GigabitEthernet 0/8

Vous pouvez avoir un total de 10 interfaces lorsque vous déployez l'ASAv. Pour les interfaces de données, assurez-vous que les réseaux sources correspondent aux réseaux de destination appropriés et que chaque interface de données est mappée à un sous-réseau ou à un VLAN unique. Vous ne devez pas utiliser toutes les interfaces; pour les interfaces que vous n'avez pas l'intention d'utiliser, elles peuvent rester désactivées dans la configuration.

Étape 11 Sur la page **Properties** (Propriétés), définissez les propriétés configurables par l'utilisateur fournies avec le modèle OVF (modèles VI uniquement) :

- **Password** (Mot de passe) : définissez le mot de passe pour l'accès administrateur.
- **Network** (Réseau) : définissez les renseignements sur le réseau, notamment le nom de domaine complet (FQDN), le DNS, le domaine de recherche et le protocole de réseau (IPv4 ou IPv6).
- **Management Interface** (Interface de gestion) : définissez la configuration de gestion, puis cliquez sur le bouton déroulant pour sélectionner **DHCP/Manual** (DHCP/Manuel) et définissez la configuration IP pour l'interface de gestion.
- **Firewall Mode** (Mode pare-feu) : définissez le mode initial du pare-feu. Cliquez sur la flèche de la liste déroulante **Firewall Mode** (Mode pare-feu) et choisissez l'un des deux modes pris en charge, **Routed (Routé) ou Transparent**.

Étape 12 Cliquez sur **NEXT** (SUIVANT). Dans la section **Ready to Complete** (Prêt à terminer), passez en revue et vérifiez les renseignements affichés. Pour commencer le déploiement avec ces paramètres, cliquez sur **Finish** (Terminer). Pour apporter des modifications, cliquez sur **Back** (Retour) pour accéder aux boîtes de dialogue précédentes.

(Facultatif) cochez l'option **Power on after deployment** (Mise sous tension après le déploiement) pour démarrer la machine virtuelle, puis cliquez sur **Finish** (Terminer).

Après avoir terminé l'assistant, le client web vSphere traite la machine virtuelle; vous pouvez voir l'état de déploiement Initialize OVF (Initialiser OVF) dans le volet **Recent Tasks** (Tâches récentes) de la zone **Global Information** (Renseignements généraux).

Lorsqu'il a terminé, vous voyez l'état d'achèvement du déploiement du modèle OVF.

L'instance ASAv apparaît dans le centre de données spécifié dans l'inventaire. Le démarrage de la nouvelle machine virtuelle (VM) peut prendre jusqu'à 30 minutes.

Remarque
Vous avez besoin d'un accès Internet pour enregistrer avec succès l'ASAv HyperFlex auprès de l'autorité de licence de Cisco. Vous devrez peut-être effectuer une configuration supplémentaire après le déploiement pour obtenir un accès Internet et un enregistrement de licence réussi.

Accéder à la console ASAv

Dans certains cas, avec ASDM, vous devrez peut-être utiliser l'interface de ligne de commande pour le dépannage. Par défaut, vous pouvez accéder à la console VMware vSphere intégrée. Vous pouvez également configurer une console série de réseau, qui a de meilleures capacités, notamment pour copier et coller.

- Utiliser la console VMware vSphere
- Configurer un port de console de série de réseau

Utiliser la console VMware vSphere

Pour la configuration initiale ou le dépannage, accédez à l'interface de ligne de commande à partir de la console virtuelle fournie par l'intermédiaire du client web VMware vSphere. Vous pourrez configurer ultérieurement l'accès à distance à l'interface de ligne de commande pour Telnet ou SSH.

Avant de commencer

Pour le client web vSphere, installez le module d'intégration de client, qui est requis pour l'accès à la console ASA virtuel.

Procédure

Étape 1 Dans le client web VMware vSphere, cliquez avec le bouton droit sur l'instance ASA virtuel dans l'inventaire et choisissez **Open Console** (Ouvrir la console). Vous pouvez également cliquer sur **Launch Console** (Lancer la console) sous l'onglet Summary (Résumé).

Étape 2 Cliquez dans la console et appuyez sur **Enter** (Entrée). Remarque : appuyez sur **Ctrl + Alt** pour libérer le curseur.

Si l'ASA virtuel démarre toujours, des messages de démarrage s'affichent.

Lorsque l'ASA virtuel démarre pour la première fois, il lit les paramètres fournis par le fichier OVF et les ajoute à la configuration système ASA virtuel. Il reprend ensuite automatiquement le processus de démarrage jusqu'à ce qu'il soit opérationnel. Ce processus de double démarrage se produit uniquement lorsque vous déployez l'ASA virtuel pour la première fois.

Remarque
Jusqu'à ce que vous installiez une licence, le débit est limité à 100 kbit/s afin que vous puissiez effectuer des tests de connectivité préalables. Une licence est requise pour le fonctionnement normal. Vous voyez également les messages suivants répétés sur la console jusqu'à ce que vous installiez une licence :

```
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.
```

L'invite suivante s'affiche :

```
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.

Exemple :

```
ciscoasa> enable
```

Le message suivant s'affiche :

```
Password:
```

Étape 4 Appuyez sur la touche **Enter** (Entrée) pour continuer. Par défaut, le champ du mot de passe est vide. Si vous avez déjà défini un mot de passe d'activation, saisissez-le au lieu d'appuyer sur Enter (Entrée).

L'invite passe à :

```
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 5 Accédez au mode de configuration globale :

```
ciscoasa# configure terminal
```

L'invite change comme suit :

```
ciscoasa(config)#
```

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

Configurer un port de console de série de réseau

Pour une meilleure expérience de la console, vous pouvez configurer un port série réseau individuellement ou relié à un concentrateur de port série virtuel (vSPC) pour l'accès à la console. Consultez la documentation de VMware vSphere pour en savoir plus sur chaque méthode. Sur l'ASA virtuel, vous devez envoyer la sortie de la console à un port série plutôt qu'à la console virtuelle. Cette procédure décrit comment activer la console de port série.

Procédure

Étape 1 Configurez un port série réseau dans VMware vSphere. Consultez la documentation de VMware vSphere.

Étape 2 Sur l'ASA virtuel, créez un fichier appelé « use_ttyS0 » dans le répertoire racine de disk0. Ce fichier n'a pas besoin d'avoir du contenu; il doit simplement exister à cet emplacement :

disk0 :/use_ttyS0

- À partir d'ASDM, vous pouvez charger un fichier texte vide portant ce nom à l'aide de la boîte de dialogue **Tools (Outils)** > **File Management (Gestion des fichiers)**.
- Au niveau de la console vSphere, vous pouvez copier un fichier existant (n'importe quel fichier) dans le système de fichiers sous le nouveau nom. Par exemple :

```
ciscoasa(config)# cd coredumpinfo
ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
```

Étape 3 Rechargez l'ASA virtuel.

- Dans ASDM, choisissez **Tools (Outils)** > **System Reload (Recharger le système)**.
- Dans la console vSphere, saisissez **reload** (recharger).

  L'ASA virtuel arrête l'envoi à la console vSphere et l'envoie plutôt à la console série.

Étape 4 Utilisez Telnet à l'adresse IP de l'hôte vSphere et au numéro de port que vous avez spécifié lorsque vous avez ajouté le port série; ou utilisez Telnet à l'adresse IP et au port vSPC.

Mettre à niveau la licence vCPU ou de débit

L'ASAv utilise une licence de débit, qui a une incidence sur le nombre de vCPU que vous pouvez utiliser.

Si vous souhaitez augmenter (ou diminuer) le nombre de vCPU pour votre ASAv, vous pouvez demander une nouvelle licence, appliquer la nouvelle licence et modifier les propriétés de la VM dans VMware pour qu'elles correspondent aux nouvelles valeurs.

Remarque Les vCPU attribués doivent correspondre à la licence vCPU ou à la licence de débit d'ASAv. La mémoire RAM doit également être de taille appropriée pour les vCPU. Lors de la mise à niveau ou de la rétrogradation, assurez-vous de suivre cette procédure et de rapprocher la licence et les vCPU immédiatement. L'ASAv ne fonctionne pas correctement en cas d'incompatibilité persistante.

Procédure

Étape 1 Demandez une nouvelle licence de vCPU ou une nouvelle licence de débit d'ASAv.

Étape 2 Appliquez la nouvelle licence. Pour les paires de basculement, appliquez de nouvelles licences aux deux unités.

Étape 3 Effectuez l'une des opérations suivantes, selon que vous utilisez le basculement ou non :

- Basculement : dans le client web vSphere, éteignez l'ASAv en mode veille. Par exemple, cliquez sur l'ASAV, puis sur **Power Off the virtual machine**(Éteindre la machine virtuelle) ou cliquez avec le bouton droit sur l'ASAv et choisissez **Shut Down Guest OS** (Arrêter le système d'exploitation invité).
- Pas de basculement : dans le client web vSphere, éteignez l'ASAv. Par exemple, cliquez sur l'ASAV, puis sur **Power Off the virtual machine**(Éteindre la machine virtuelle) ou cliquez avec le bouton droit sur l'ASAv et choisissez **Shut Down Guest OS** (Arrêter le système d'exploitation invité).

Étape 4 Cliquez sur l'ASAv, puis sur **Edit Virtual machine settings** (Modifier les paramètres de la machine virtuelle) (ou cliquez avec le bouton droit sur l'ASAv et choisissez **Edit Settings** (Modifier les paramètres)).

La boîte de dialogue **Edit Settings** (Modifier les paramètres) s'affiche.

Étape 5 Reportez-vous aux exigences de CPU et de mémoire dans Gestion des licences pour l'ASA virtuel, à la page 1 pour déterminer les valeurs correctes pour la nouvelle licence vCPU.

Étape 6 Sous l'onglet **Virtual Hardware** (Matériel virtuel), pour le **CPU**, choisissez la nouvelle valeur dans la liste déroulante.

Étape 7 Pour **Memory** (Mémoire), entrez la nouvelle valeur de la mémoire RAM.

Étape 8 Cliquez sur **OK**.

Étape 9 Mettez l'ASAv sous tension. Par exemple, cliquez sur **Power On the Virtual Machine** (Mettre la machine virtuelle sous tension).

Étape 10 Pour les paires de basculement :

1. Ouvrez une console à l'unité active ou lancez ASDM sur l'unité active.
2. Une fois que l'unité en mode veille a fini de démarrer, basculez vers l'unité en mode veille :
   - ASDM : choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Faillover (Basculement)** > **Status (État)**, et cliquez sur **Make Standby** (Mettre en veille).

- Interface de ligne de commande : **failover active**

3. Répétez les étapes 3 à 9 pour l'unité active.

Prochaine étape

Consultez Gestion des licences pour l'ASA virtuel, à la page 1 pour de plus amples renseignements.

Réglage de la performance

L'ASAv est un appareil à haute performance, mais peut nécessiter l'ajustement de Cisco HyperFlex pour obtenir les meilleurs résultats.

Voici des bonnes pratiques et des recommandations pour améliorer les performances de l'ASAv dans un environnement HyperFlex.

Activation des trames étendues

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 d'ASAv 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 bâtis grand format : vous pouvez définir la MTU à 9 198 octets maximum. Le maximum est de 9 000 pour l'ASAv.

Cette procédure explique comment activer les bâtis grand format dans l'environnement suivant :

HyperFlex Cluster on the vSphere 7.0.1 (Grappe HyperFlex sur vSphere 7.0.1) > **VMware vSphere vSwitch**> **Cisco UCS Fabric Interconnects (FI) (Interconnexions de trames Cisco UCS).**

Procédure

Étape 1 Modifiez les paramètres MTU de l'hôte ASAv sur lequel vous avez déployé l'ASAv.

1. Connectez-vous au serveur vCenter à l'aide du client web vSphere.
2. Dans les **Advanced System Settings** (Paramètres système avancés) de votre hôte HyperFlex, définissez la valeur du paramètre de configuration`Net.Vmxnet3NonTsoPacketGtMtuAllowed` sur `1`.
3. Enregistrez les modifications et redémarrez l'hôte.

Pour en savoir plus, consultez https://kb.vmware.com/s/article/1038578.

Étape 2 Modifiez les paramètres MTU de VMware vSphere vSwitch.

1. Connectez-vous au serveur vCenter à l'aide du client web vSphere.

2. Modifiez les propriétés de VMware vSphere vSwitch et définissez la valeur de la **MTU** à `9 000`.

Étape 3 Modifiez les paramètres MTU de Cisco UCS Fabric Interconnects (FI).

1. Connectez-vous à la console de gestion Cisco UCS.
2. Pour modifier la classe du système QoS, sélectionnez **LAN** > **LAN Cloud (Nuage LAN)** > **QoS System Class (Classe du système QoS).** Sous l'onglet **General (Général)**, définissez la valeur de la **MTU** à 9 216.
3. Pour modifier votre vNIC, choisissez **LAN** > **Policies (Politiques)** > **racine (racine)** > **Sub-Organisations (Sous-organisations)**

   <your-hyperflex-org>**vNIC Templates (Modèles vNIC)**<your-vnic>. Sous l'onglet **General (Général)**, définissez la valeur de la **MTU** à 9 000.

CHAPITRE 17

Configurer l'ASA virtuel

Le déploiement ASA virtuel préconfigure l'accès ASDM. À partir de l'adresse IP client que vous avez spécifiée lors du déploiement, vous pouvez vous connecter à la gestion des adresses IP de l'ASA virtuel à l'aide d'un navigateur Web. Ce chapitre décrit également comment autoriser d'autres clients à accéder à ASDM et comment autoriser l'accès à l'interface de ligne de commande (SSH ou Telnet). D'autres tâches de configuration essentielles traitées dans ce chapitre comprennent l'installation de la licence et les tâches de configuration courantes fournies par les assistants dans ASDM.

- Démarrer ASDM, à la page 319
- Effectuer la configuration initiale à l'aide d'ASDM , à la page 320
- Configuration avancée, à la page 322

Démarrer ASDM

Procédure

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

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

La fenêtre de lancement ASDM apparaît avec les boutons suivants :

- **Installer le lanceur ASDM et exécuter ASDM**
- **Exécuter ASDM**
- **Exécuter l'assistant de démarrage**

Étape 2 Pour télécharger le lanceur :

a) Cliquez sur **Install ASDM Launcher and Run ASDM** (Installer le lanceur ASDM et exécuter 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. Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé.

c) Enregistrez le programme d'installation sur votre PC, 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, laissez le nom d'utilisateur et le mot de passe vides (pour une nouvelle installation), puis cliquez sur **OK**. Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé.

Étape 3 Pour utiliser Java Web Start :

a) Cliquez **Run ASDM** (Exécuter ASDM) ou **Run Startup Wizard** (Exécuter l'assistant de démarrage).
b) Enregistrez le raccourci sur votre ordinateur lorsque vous y êtes invité(e). Vous pouvez également l'ouvrir au lieu de l'enregistrer.
c) Démarrez Java Web Start à partir du raccourci.
d) Acceptez tous les certificats en fonction des boîtes de dialogue qui s'affichent. Le lanceur Cisco ASDM-IDM apparaît.
e) Laissez le nom d'utilisateur et le mot de passe vides (pour une nouvelle installation), puis cliquez sur **OK**. Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé.

Effectuer la configuration initiale à l'aide d'ASDM

Vous pouvez effectuer la configuration initiale en utilisant les assistants et les procédures ASDM suivants.

- Exécuter l'assistant de démarrage
- (Facultatif) Autoriser l'accès aux serveurs publics derrière l'ASA virtuel
- (Facultatif) Exécuter les assistants de réseau privé virtuel (VPN)
- (Facultatif) Exécuter d'autres assistants dans ASDM

Pour la configuration de l'interface de ligne de commande, consultez les guides de configuration de la CLI de la série Cisco Cisco Secure Firewall ASA .

Exécuter l'assistant de démarrage

Exécutez l'**assistant de démarrage** pour personnaliser la politique de sécurité en fonction de votre déploiement.

Procédure

Étape 1 Choisissez **Wizards (assistants)** > **Startup Wizard (assistant de démarrage)**.

Étape 2 Personnalisez la politique de sécurité en fonction de votre déploiement. Vous pouvez définir les éléments suivants :

- Nom d'hôte
- Nom de domaine
- Mot de passe administratif
- Interfaces
- Adresses IP
- du routage statique;

- Serveur DHCP
- Règles de traduction d'adresse réseau
- et plus encore…

(Facultatif) Autoriser l'accès aux serveurs publics derrière l'ASA virtuel

Le volet **Configuration** > **Firewall (Pare-feu)** > **Public Servers (Serveurs publics)** configure automatiquement la politique de sécurité pour rendre un serveur interne accessible à partir d'Internet. En tant que propriétaire d'entreprise, vous pouvez avoir des services de réseau interne, tels qu'un serveur web et FTP, qui doivent être disponibles pour un utilisateur externe. Vous pouvez placer ces services sur un réseau distinct derrière l'ASA virtuel, appelé zone démilitarisée (DMZ). En plaçant les serveurs publics sur DMZ, les attaques lancées contre les serveurs publics n'affectent pas vos réseaux internes.

(Facultatif) Exécuter les assistants de réseau privé virtuel (VPN)

Vous pouvez configurer le réseau privé virtuel (VPN) à l'aide des assistants suivants (**Wizards (assistants)** > **VPN Wizards (assistants VPN)**) :

- Site-to-Site VPN Wizard (assistant VPN de site à site) : crée un tunnel IPsec de site à site entre l'ASA virtuel et un autre périphérique compatible avec le réseau privé virtuel (VPN).
- AnyConnect VPN Wizard (assistant VPN AnyConnect) : configure l'accès à distance au réseau privé virtuel (VPN) SSL pour Cisco AnyConnect VPN client. client AnyConnect fournit des connexions SSL sécurisées à l'ASA pour les utilisateurs distants avec une tunnellisation VPN complète aux ressources de l'entreprise. Vous pouvez configurer la politique ASA pour télécharger l'client AnyConnect pour les utilisateurs distants lorsqu'ils se connectent pour la première fois par le biais d'un navigateur. Avec client AnyConnect 3.0 et les versions ultérieures, le client peut exécuter le protocole VPN SSL ou IPsec IKEv2.
- Clientless SSL VPN Wizard (assistant VPN SSL sans client) : configure l'accès à distance au VPN SSL sans client pour un navigateur. Le VPN SSL sans client et par navigateur permet aux utilisateurs d'établir un tunnel VPN sécurisé d'accès à distance vers l'ASA à l'aide d'un navigateur Web. Après l'authentification, les utilisateurs accèdent à une page de portail et peuvent accéder à des ressources internes spécifiques prises en charge. L'administrateur réseau fournit un accès aux ressources par les utilisateurs par groupe. Les listes de contrôle d'accès peuvent être appliquées pour restreindre ou autoriser l'accès à des ressources d'entreprise spécifiques.
- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard (assistant VPN d'accès à distance IPsec (IKEv1 ou IKEv2) : configure l'accès à distance du VPN IPsec pour le client Cisco IPsec.

Pour plus d'informations sur la configuration d'une connexion ASA virtuel IPsec Virtual Tunnel Interface (VTI) à Azure, consultez Configurer la connexion ASA IPsec VTI à Azure.

(Facultatif) Exécuter d'autres assistants dans ASDM

Vous pouvez exécuter d'autres assistants dans ASDM pour configurer le basculement avec la haute disponibilité, l'équilibrage de charges des grappes VPN et la capture de paquets.

- Assistant de haute disponibilité et d'évolutivité : configurez le basculement ou l'équilibrage de charges VPN.
- Assistant de capture de paquets : configurez et exécutez la capture de paquets. L'assistant exécute une capture de paquets sur chacune des interfaces d'entrée et de sortie. Après avoir capturé des paquets, vous pouvez enregistrer les captures de paquets sur votre PC pour les examiner et les relire dans l'analyseur de paquets.

Configuration avancée

Pour poursuivre la configuration de votre ASA virtuel, consultez la documentation Naviguer dans la série Cisco Secure Firewall ASA.

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.