Mode contexte multiple

Ce chapitre décrit comment configurer plusieurs contextes de sécurité sur l'ASA.

À propos des contextes de sécurité

Vous pouvez partitionner un ASA unique en plusieurs périphériques virtuels, appelés contextes de sécurité. Chaque contexte agit comme un périphérique indépendant, avec sa politique de sécurité, ses interfaces et ses administrateurs. Les contextes multiples sont similaires au fait d'avoir plusieurs périphériques autonomes. Pour les fonctionnalités non prises en charge en mode de contexte multiple, consultez Lignes directrices pour le mode de contexte multiple, à la page 14.

Cette section fournit un aperçu des contextes de sécurité.

Utilisations courantes des contextes de sécurité

Vous pouvez utiliser plusieurs contextes de sécurité dans les situations suivantes :

- Vous êtes un fournisseur de services et vous souhaitez vendre des services de sécurité à de nombreux clients. En activant plusieurs contextes de sécurité sur l'ASA, vous pouvez mettre en œuvre une solution économique et peu encombrante qui sépare et sécurise tout le trafic client, tout en facilitant la configuration.
- Vous êtes une grande entreprise ou un campus universitaire et souhaitez séparer complètement les services.
- Vous êtes une entreprise qui souhaite fournir des politiques de sécurité distinctes à différents services.
- Vous avez un réseau qui nécessite plusieurs ASA.

Fichiers de configuration de contexte

Cette section décrit comment l'ASA met en œuvre les configurations en mode de contexte multiple.

Configurations de contexte

Pour chaque contexte, l'ASA comprend une configuration qui identifie la politique de sécurité, les interfaces et toutes les options que vous pouvez configurer sur un périphérique autonome. Vous pouvez stocker les configurations de contexte dans la mémoire flash ou vous pouvez les télécharger à partir d'un serveur TFTP, FTP ou HTTP(S).

Configuration système

L'administrateur du système ajoute et gère les contextes en configurant chaque emplacement de configuration de contexte, les interfaces allouées et d'autres paramètres de fonctionnement de contexte dans la configuration système, qui, à l'instar d'une configuration monomode, est la configuration de démarrage. La configuration système identifie les paramètres de base de l'ASA. La configuration système n'inclut aucune interface réseau ni aucun paramètre réseau pour elle-même; au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise l'un des contextes désigné comme *contexte d'administration*. La configuration système comprend une interface de basculement spécialisée pour le trafic de basculement uniquement.

Configuration du contexte d'administration

Le contexte d'administration est similaire à tout autre contexte, sauf que lorsqu'un utilisateur se connecte au contexte d'administration, cet utilisateur dispose de droits d'administrateur système et peut accéder au système et à tous les autres contextes. Le contexte admin n'est limité en aucune façon et peut être utilisé comme contexte standard. Cependant, comme la connexion au contexte admin vous accorde des privilèges d'administrateur sur tous les contextes, vous devrez peut-être restreindre l'accès au contexte admin aux utilisateurs appropriés. Le contexte d'administration doit résider dans la mémoire flash et non à distance.

Si votre système est déjà en mode de contexte multiple, ou si vous effectuez une conversion à partir du mode unique, le contexte d'administration est automatiquement créé sous la forme d'un fichier sur la mémoire flash interne, appelé admin.cfg. Ce contexte s'appelle « admin ». Si vous ne souhaitez pas utiliser admin.cfg comme contexte d'administration, vous pouvez modifier le contexte d'administration.

Classement des paquets par l'ASA

Chaque paquet qui entre dans le châssis doit être classé par l'ASA, de sorte que ce dernier puisse déterminer à quel contexte envoyer un paquet.

Remarque Si l'adresse MAC de destination est une adresse MAC de multidiffusion ou de diffusion, le paquet est dupliqué et remis à chaque contexte.

Critères de classificateurs valides

Cette section décrit les critères utilisés par le classificateur.

Remarque Pour le trafic de gestion destiné à une interface, l'adresse IP de l'interface est utilisée pour la classification.

La table de routage n'est pas utilisée pour la classification des paquets.

Interfaces uniques

Si un seul contexte est associé à l'interface d'entrée, l'ASA classe le paquet dans ce contexte. En mode de pare-feu transparent, des interfaces uniques pour les contextes sont requises. Cette méthode est donc utilisée pour classer les paquets à tout moment.

Adresses MAC uniques

Si plusieurs contextes partagent une interface, le classificateur utilise des adresses MAC uniques attribuées à l'interface dans chaque contexte. Un routeur en amont ne peut pas acheminer directement vers un contexte sans adresse MAC unique. Vous pouvez activer la génération automatique des adresses MAC. Vous pouvez également définir les adresses MAC manuellement lorsque vous configurez chaque interface.

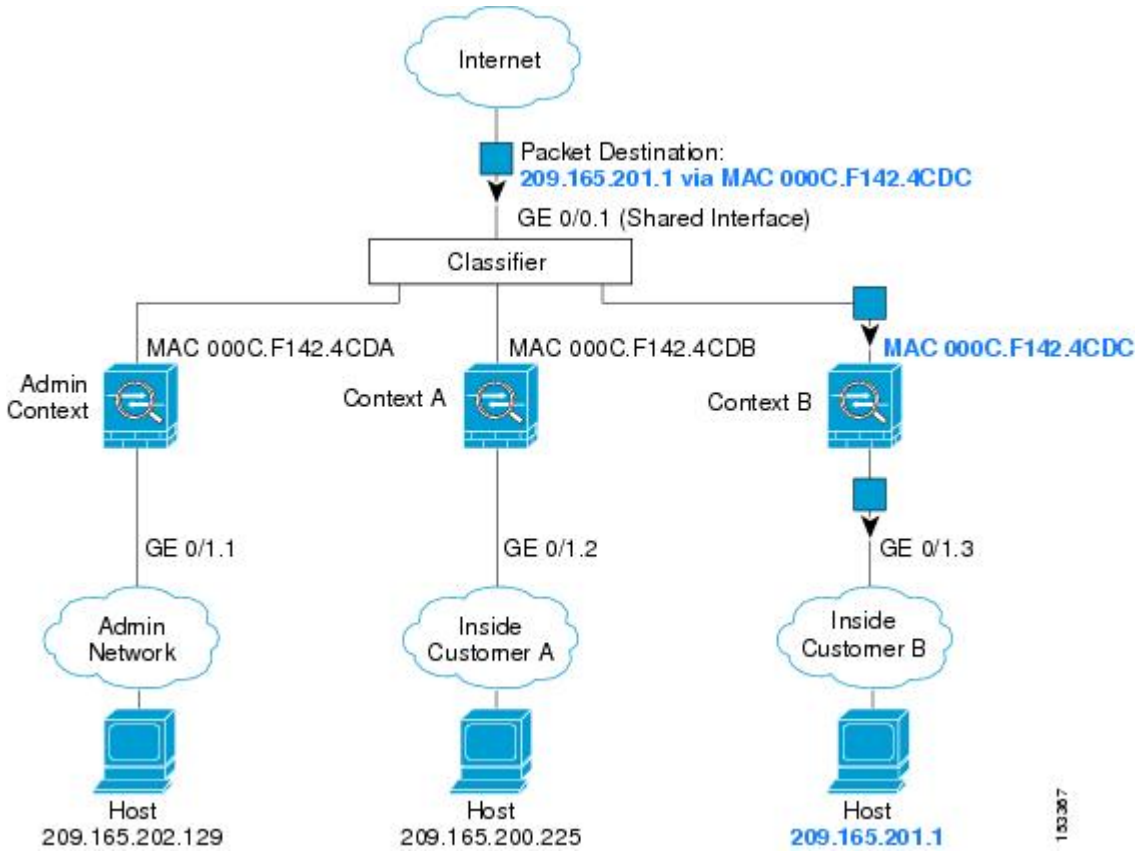
Configuration NAT

Si vous n'activez pas l'utilisation d'adresses MAC uniques, l'ASA utilise les adresses mappées dans votre configuration NAT pour classer les paquets. Nous vous conseillons d'utiliser des adresses MAC au lieu de NAT afin que la classification du trafic puisse avoir lieu indépendamment de l'exhaustivité de la configuration NAT.

Exemples de classement

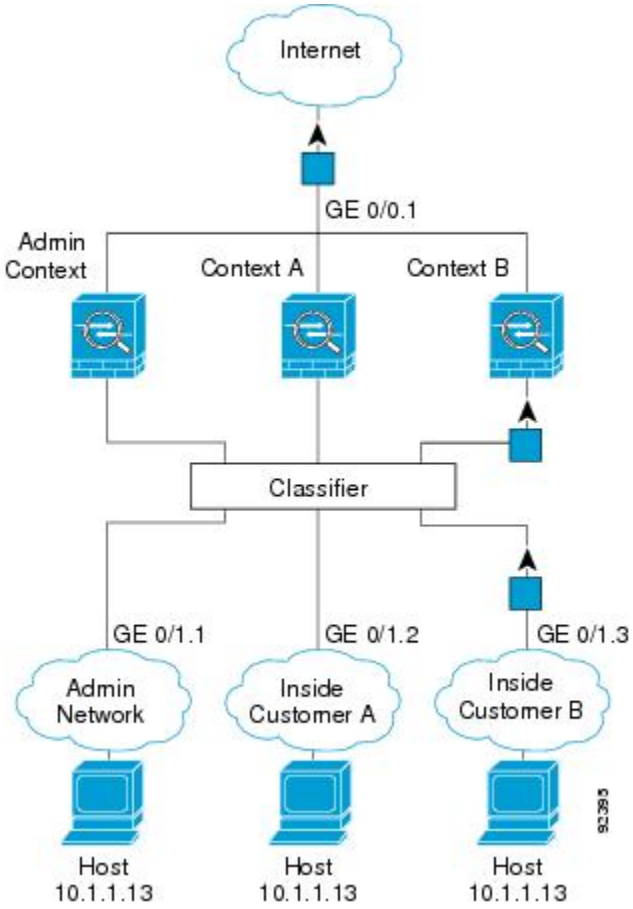
La figure suivante montre plusieurs contextes partageant une interface externe. Le classificateur affecte le paquet au contexte B, car le contexte B comprend l'adresse MAC à laquelle le routeur envoie le paquet.

Illustration 1 : Classification des paquets avec une interface partagée à l'aide d'adresses MAC



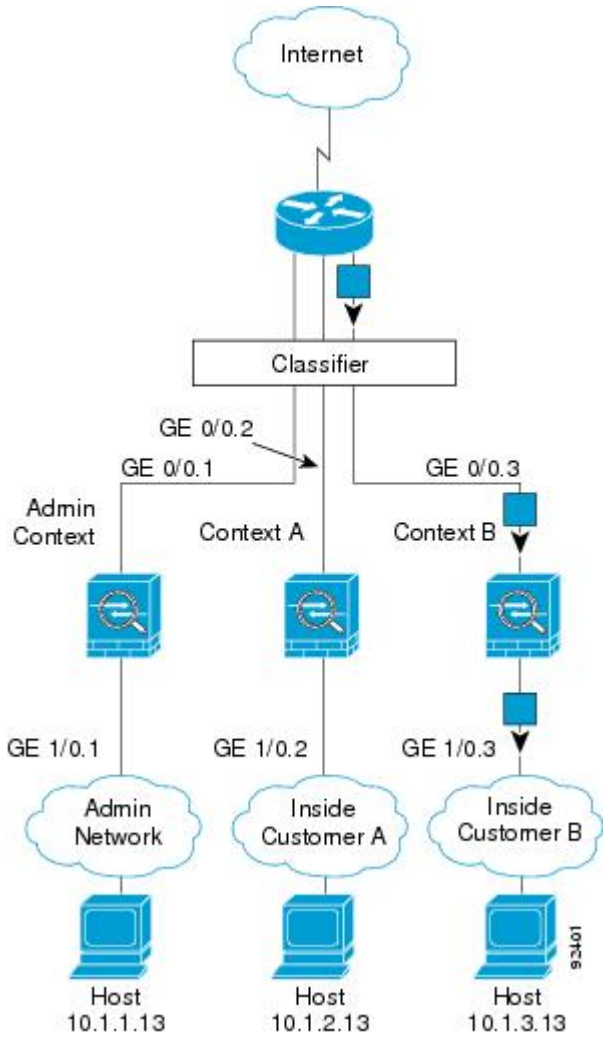
Notez que tout nouveau trafic entrant doit être classé, même en provenance des réseaux internes. La figure suivante montre un hôte sur le réseau interne du contexte B qui accède à Internet. Le classificateur affecte le paquet au contexte B, car l'interface d'entrée est Gigabit Ethernet 0/1.3, qui est affectée au contexte B.

Illustration 2 : Trafic entrant des réseaux internes



Pour les pare-feu transparents, vous devez utiliser des interfaces uniques. La figure suivante montre un paquet destiné à un hôte du contexte B à partir d'Internet. Le classificateur affecte le paquet au contexte B, car l'interface d'entrée est Gigabit Ethernet 1/0.3, qui est affectée au contexte B.

Illustration 3 : Contextes de pare-feu transparent



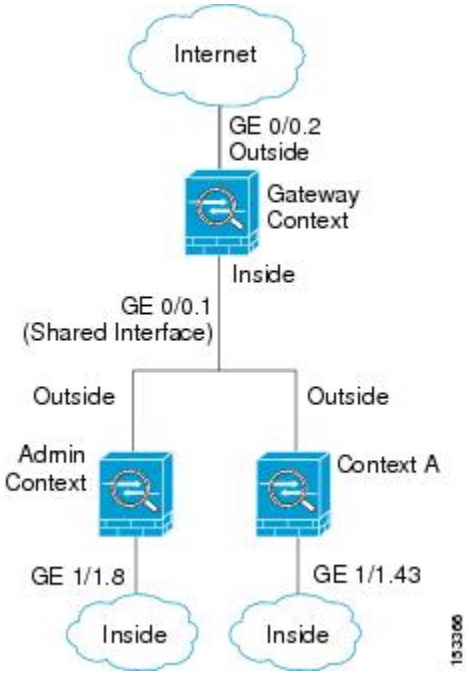
Contextes de sécurité en cascade

Le fait de placer un contexte directement devant un autre contexte s'appelle *des contextes en cascade*; l'interface externe d'un contexte est la même interface que l'interface interne d'un autre contexte. Vous pourriez souhaiter mettre des contextes en cascade si vous souhaitez simplifier la configuration de certains contextes en configurant des paramètres partagés dans le contexte supérieur.

Remarque La mise en cascade des contextes nécessite des adresses MAC uniques pour chaque interface de contexte. En raison des limites de la classification des paquets sur des interfaces partagées sans adresses MAC, nous vous conseillons de ne pas utiliser de contextes de chaîne de caractères sans adresses MAC uniques.

La figure suivante montre un contexte de passerelle avec deux contextes derrière la passerelle.

Illustration 4 : Contextes en cascade



Accès de gestion aux contextes de sécurité

L'ASA fournit un accès administrateur de système en mode de contexte multiple ainsi qu'un accès pour les administrateurs de contexte individuel.

Accès à l'administrateur système

Vous pouvez accéder à l'ASA en tant qu'administrateur système de deux manières :

- Accédez à la console ASA.

  À partir de la console, vous accédez à l'*espace d'exécution du système*, ce qui signifie que toutes les commandes que vous saisissez n'affectent que la configuration ou le fonctionnement du système (pour les commandes d'exécution).

- Accédez au contexte d'administration à l'aide de Telnet, SSH ou ASDM.

En tant qu'administrateur système, vous pouvez accéder à tous les contextes.

L'espace d'exécution du système ne prend en charge aucune commande AAA, mais vous pouvez configurer son propre mot de passe d'activation, ainsi que ses noms d'utilisateur dans la base de données locale pour fournir des connexions individuelles.

Accès à l'administrateur de contexte

Vous pouvez accéder à un contexte en utilisant Telnet, SSH ou ASDM. Si vous vous connectez à un contexte de non-administration, vous pouvez uniquement accéder à la configuration de ce contexte. Vous pouvez fournir des identifiants individuels pour le contexte.

Utilisation de l'interface de gestion

L’interface de gestion est une interface distincte uniquement pour le trafic de gestion.

En mode de pare-feu routé, vous pouvez partager l'interface de gestion dans tous les contextes.

En mode de pare-feu transparent, l'interface de gestion est spéciale. En plus du nombre maximal d’interfaces de trafic traversant autorisé, vous pouvez également utiliser l’interface de gestion en tant qu’interface de gestion uniquement distincte. Cependant, en mode contexte multiple, vous ne pouvez pas partager d’interfaces entre des contextes transparents. Vous pouvez plutôt utiliser les sous-interfaces de l’interface de gestion et en affecter une à chaque contexte. Cependant, seuls les modèles de périphérique Firepower autorisent les sous-interfaces sur l’interface de gestion. Pour les modèles d’ASA, vous devez utiliser une interface de données ou une sous-interface d’une interface de données et l’ajouter à un groupe de ponts dans le contexte.

Pour le contexte transparent Châssis Firepower 4100/9300 , ni l’interface de gestion ni la sous-interface ne conservent leur état spécial. Dans ce cas, vous devez la traiter comme une interface de données et l'ajouter à un groupe de ponts. (Notez qu’en mode contexte unique, l’interface de gestion conserve son état spécial.)

Une autre considération à propos du mode transparent : lorsque vous activez le mode à contextes multiples, toutes les interfaces configurées sont automatiquement affectées au contexte Admin. Par exemple, si votre configuration par défaut comprend l’interface de gestion, cette interface sera affectée au contexte d’administration. Une option consiste à laisser l’interface principale allouée au contexte d’administration et à la gérer à l’aide du VLAN natif, puis d’utiliser des sous-interfaces pour gérer chaque contexte. Gardez à l’esprit que si vous rendez le contexte d’administration transparent, son adresse IP sera supprimée. vous devez l’affecter à un groupe de ponts et affecter l’adresse IP aux BVI.

À propos de la gestion des ressources

Par défaut, tous les contextes de sécurité ont un accès illimité aux ressources de l’ASA, sauf lorsque des limites maximales par contexte sont appliquées; la seule exception concerne les ressources du VPN, qui sont désactivées par défaut. Si vous trouvez qu’un ou plusieurs contextes utilisent trop de ressources et qu’ils entraînent le refus de connexion à d’autres contextes, par exemple, vous pouvez configurer la gestion des ressources pour limiter l’utilisation des ressources par contexte. Pour les ressources VPN, vous devez configurer la gestion des ressources pour autoriser tous les tunnels VPN.

Classes des ressources

L’ASA gère les ressources en attribuant des contextes aux classes de ressources. Chaque contexte utilise les limites de ressources définies par la classe. Pour utiliser les paramètres d’une classe, affectez le contexte à la classe lorsque vous définissez le contexte. Tous les contextes appartiennent à la classe par défaut s’ils ne sont pas affectés à une autre classe; vous n’avez pas à attribuer activement un contexte à la classe par défaut. Vous ne pouvez affecter un contexte qu’à une seule classe de ressources. L’exception à cette règle est que les limites non définies dans la classe membre sont héritées de la classe par défaut; ainsi, un contexte peut être membre de la classe par défaut et d’une autre classe.

Limites des ressources

Vous pouvez définir la limite des ressources individuelles en pourcentage (s’il y a une limite de système matériel) ou en tant que valeur absolue.

Pour la plupart des ressources, l’ASA ne réserve pas une partie des ressources pour chaque contexte attribué à la classe; au lieu de cela, l’ASA définit la limite maximum pour un contexte. Si vous dépassez les ressources ou si vous permettez à certaines ressources d’être illimitées, quelques contextes peuvent « utiliser » ces ressources, ce qui peut affecter le service fourni à d’autres contextes. L’exception concerne les types de

ressources VPN, que vous ne pouvez pas dépasser, de sorte que les ressources attribuées à chaque contexte sont garanties. Pour prendre en charge des rafales temporaires de sessions VPN au-delà de la quantité attribuée, l'ASA prend en charge un type de ressource VPN en « rafale », qui est égal au nombre de sessions VPN non attribuées restantes. Les sessions en rafale *peuvent* être surexploitées et sont disponibles pour les contextes selon le principe du premier arrivé premier servi.

Classe par défaut

Tous les contextes appartiennent à la classe par défaut s'ils ne sont pas affectés à une autre classe; vous n'avez pas besoin d'affecter activement un contexte à la classe par défaut.

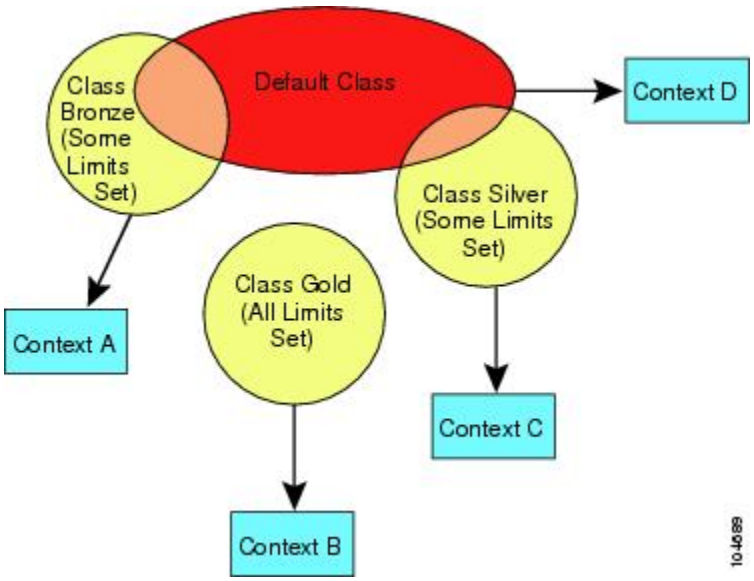
Si un contexte appartient à une autre classe que la classe par défaut, les paramètres de cette classe remplacent toujours les paramètres de la classe par défaut. Cependant, si l'autre classe a des paramètres non définis, le contexte membre utilise la classe par défaut pour ces limites. Par exemple, si vous créez une classe avec une limite de 2 % pour toutes les connexions simultanées, mais aucune autre limite, toutes les autres limites sont héritées de la classe par défaut. Inversement, si vous créez une classe avec une limite pour toutes les ressources, la classe n'utilise aucun paramètre de la classe par défaut.

Pour la plupart des ressources, la classe par défaut fournit un accès illimité aux ressources pour tous les contextes, sauf pour les limites suivantes :

- Sessions Telnet—5 sessions. (Le maximum par contexte.)
- Sessions SSH—5 sessions. (Le maximum par contexte.)
- Sessions ASDM—5 sessions. (Le maximum par contexte.)
- Adresses MAC—(selon le modèle). (Le maximum pour le système.)
- Secure Client (services client sécurisés) homologues—0 session. (Vous devez configurer manuellement la classe pour autoriser tous les homologues Secure Client (services client sécurisés).)
- Tunnels VPN de site à site—0 session. (Vous devez configurer manuellement la classe pour autoriser toutes les sessions VPN.)

La figure suivante montre la relation entre la classe par défaut et les autres classes. Les contextes A et C appartiennent à des classes avec des limites définies; les autres limites sont héritées de la classe par défaut. Le contexte B n'hérite aucune limite de la valeur par défaut, car toutes les limites sont définies dans sa classe, la classe Gold. Le contexte D n'a pas été affecté à une classe et est, par défaut, membre de la classe par défaut.

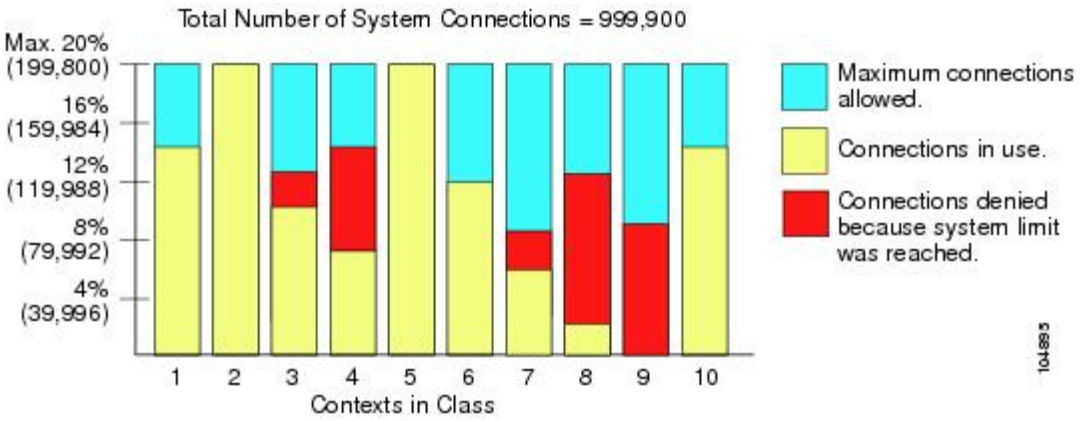
Illustration 5 : Classes des ressources



Utiliser des ressources surexploitées

Vous pouvez surabonner l'ASA en attribuant plus de 100 % d'une ressource dans tous les contextes (à l'exception des ressources VPN non rafales). Par exemple, vous pouvez définir la classe bronze pour limiter les connexions à 20 % par contexte, puis affecter 10 contextes à la classe pour un total de 200 %. Si les contextes utilisent simultanément plus que la limite du système, chaque contexte obtient moins des 20 % prévus.

Illustration 6 : Surabonnement des ressources

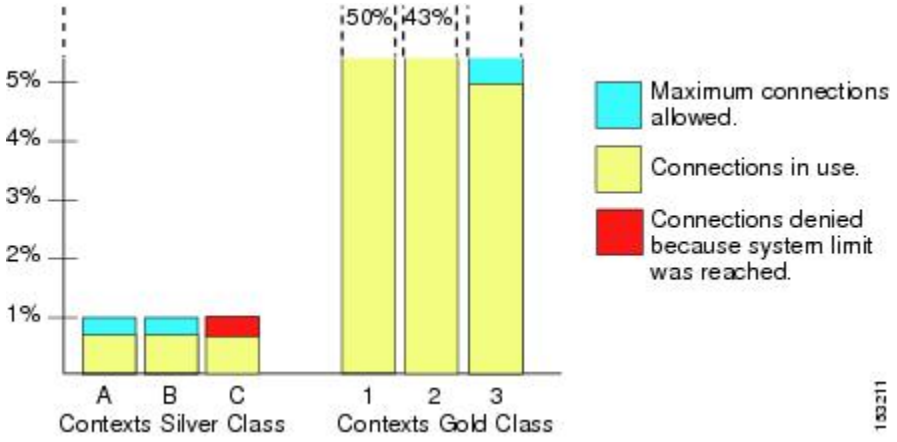


Utiliser des ressources illimitées

L'ASA vous permet d'attribuer un accès illimité à une ou plusieurs ressources dans une classe, au lieu d'un pourcentage ou d'un nombre absolu. Lorsqu'une ressource est illimitée, les contextes peuvent utiliser autant de ressources que le système en dispose. Par exemple, les contextes A, B et C appartiennent à la classe Silver, qui limite chaque membre de la classe à 1 % des connexions, pour un total de 3 %; mais les trois contextes n'utilisent actuellement que 2 % combinés. La classe Gold dispose d'un accès illimité aux connexions. Les

contextes de la classe Gold peuvent utiliser plus de 97 % des connexions « non attribuées »; ils peuvent également utiliser le 1 % de connexions non actuellement utilisées par les contextes A, B et C, même si cela signifie que les contextes A, B et C ne peuvent pas atteindre leur limite combinée de 3 %. La configuration d'un accès illimité s'apparente au surabonnement de l'ASA, à la différence que vous avez moins de contrôle sur le nombre de surabonnements du système.

Illustration 7 : Ressources illimitées



À propos des adresses MAC

Vous pouvez affecter manuellement des adresses MAC pour remplacer la valeur par défaut. Pour le mode de contexte multiple, vous pouvez générer automatiquement des adresses MAC uniques (pour toutes les interfaces affectées à un contexte) et un mode de contexte unique (pour les sous-interfaces)..

Remarque Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de liaison IPv6 sont générées sur la base de l'adresse MAC, l'attribution d'adresses MAC uniques aux sous-interfaces permet d'obtenir des adresses locales de liaison IPv6 uniques, ce qui peut éviter la perturbation du trafic dans certaines instances du périphérique ASA.

Adresses MAC en mode de contexte multiple

L'adresse MAC est utilisée pour classer les paquets dans un contexte. Si vous partagez une interface, mais que vous n'avez pas d'adresses MAC uniques pour l'interface dans chaque contexte, d'autres méthodes de classification sont tentées qui pourraient ne pas fournir une couverture complète.

Pour permettre aux contextes de partager des interfaces, vous devez activer la génération automatique d'adresses MAC virtuelles pour chaque interface de contexte partagé.

Adresses MAC automatiques

En mode de contexte multiple, la génération automatique affecte des adresses MAC uniques à toutes les interfaces affectées à un contexte.

Si vous attribuez manuellement une adresse MAC et activez la génération automatique, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée, si elle est activée.

Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC pour l'interface.

Comme les adresses générées automatiquement (lors de l'utilisation d'un préfixe) commencent par A2, vous ne pouvez pas commencer les adresses MAC manuelles par A2 si vous souhaitez également utiliser la génération automatique.

Le châssis génère l'adresse MAC en utilisant le format suivant :

A2*xx.yyzz.zzzz*

Où *xx.yy* est un préfixe défini par l'utilisateur ou un préfixe généré automatiquement en fonction des deux derniers octets de l'adresse MAC de l'interface, et *zz.zzzz* est un compteur interne généré par l'ASA. Pour l'adresse MAC de secours, l'adresse est identique, sauf que le compteur interne est augmenté de 1.

Pour donner un exemple d'utilisation du préfixe, si vous définissez le préfixe 77, l'ASA convertit 77 en valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native de l'ASA :

A2**4D.00***zz.zzzz*

Pour un préfixe 1009 (03F1), l'adresse MAC est :

A2**F1.03***zz.zzzz*

Remarque Le format d'adresse MAC sans préfixe est une version existante. Consultez la commande **mac-address auto** dans la référence de commandes pour plus d'informations sur le format existant.

Prise en charge du VPN

Pour les ressources VPN, vous devez configurer la gestion des ressources pour autoriser tous les tunnels VPN.

Vous pouvez utiliser le VPN de site à site en mode de contexte multiple.

Pour le VPN d'accès à distance, vous devez utiliser AnyConnect 3.x ou une version ultérieure pour le SSL VPN et le protocole IKEv2. Vous pouvez personnaliser le stockage flash par contexte pour les images et les personnalisations Secure Client (services client sécurisés), et utiliser la mémoire flash partagée pour tous les contextes. Pour les fonctionnalités non prises en charge, consultez Lignes directrices pour le mode de contexte multiple, à la page 14. Pour une liste détaillée des fonctionnalités VPN prises en charge par version ASA, consultez Historique du mode de contexte multiple, à la page 44.

Remarque La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante.

Licences pour le mode de contexte multiple

Modèle	Exigence de licence
Firepower 1010	Aucune assistance.
Firepower 1100	Licence Essentials : 2 contextes. *Licence facultative, maximum :* *Firepower 1120 : 5* *Firepower 1140 : 10* *Firepower 1150 : 25*
Firepower de la série 2100	Licence Essentials : 2 contextes. *Licence facultative, maximum :* *Firepower 2110 : 25* *Firepower 2120 : 25* *Firepower 2130 : 30* *Firepower 2140 : 40*
Secure Firewall 3100	Licence Essentials : 2 contextes. *Licence facultative, maximum :* *Secure Firewall 3105 : 100* *Secure Firewall 3110 : 100* *Secure Firewall 3120 : 100* *Secure Firewall 3130 : 100* *Secure Firewall 3140 : 100*
Firepower 4100	Licence Essentials : 10 contextes. *Licence facultative : jusqu'à 250 contextes.*
Firepower 9300	Licence Essentials : 10 contextes. *Licence facultative : jusqu'à 250 contextes.*
ISA 3000	Aucune assistance.
ASA virtuel	Aucune assistance.

Remarque Si le contexte d'administration ne contient que des interfaces de gestion uniquement et ne comprend aucune interface de données pour le trafic de transit, il n'est pas pris en compte dans la limite.

Remarque La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante.

Conditions préalables pour le mode de contexte multiple

Une fois que vous êtes en mode de contexte multiple, connectez-vous au système ou au contexte d'administration pour accéder à la configuration système. Vous ne pouvez pas configurer le système à partir d'un contexte de non-administration. Par défaut, après avoir activé le mode de contexte multiple, vous pouvez vous connecter au contexte d'administration en utilisant l'adresse IP de gestion par défaut.

Lignes directrices pour le mode de contexte multiple

Basculement

Le basculement en mode actif/actif n'est pris en charge qu'en mode de contexte multiple.

IPv6

Le routage IPv6 inter-contextes n'est pas pris en charge.

Fonctionnalités non prises en charge

Le mode de contexte multiple ne prend pas en charge les fonctionnalités suivantes :

- RIP
- OSPFv3. (OSPFv2 est pris en charge.)
- Routage multidiffusion
- Détection des menaces
- Communications unifiées
- Qualité de service
- Interfaces de tunnel virtuel (VTI)
- Suivi du routage statique

Le mode de contexte multiple ne prend actuellement pas en charge les fonctionnalités suivantes pour le VPN d'accès à distance :

- AnyConnect 2.x et versions antérieures
- IKEv1
- SAML
- Lancement Web

- Mise en correspondance VLAN
- Analyse de l'hôte
- Équilibrage de la charge VPN
- Personnalisation
- L2TP

Directives supplémentaires

- Le mode de contexte (unique ou multiple) n'est pas stocké dans le fichier de configuration, même s'il résiste aux redémarrages. Si vous devez copier votre configuration sur un autre périphérique, définissez le mode sur le nouveau périphérique pour qu'il corresponde.
- Si vous stockez les configurations de contexte dans le répertoire racine de la mémoire flash, sur certains modèles, vous risquez de manquer d'espace dans ce répertoire, même s'il y a de la mémoire disponible. Dans ce cas, créez un sous-répertoire pour vos fichiers de configuration. Arrière-plan : certains modèles utilisent le système de fichiers FAT 16 pour la mémoire flash interne, et si vous n'utilisez pas les noms abrégés conformes à la norme 8.3 ou les caractères majuscules, moins de 512 fichiers et dossiers peuvent être stockés parce que le système de fichiers utilise des logements pour stocker les noms de fichiers longs (voir http://support.microsoft.com/kb/120138/en-us).
- Dans ACI, le contrôle d'intégrité de la redirection basée sur les politiques (PBR) est exécuté (pings L2) en utilisant la même adresse MAC sur toutes les feuilles. Cela entraîne une oscillation MAC. Pour résoudre l'oscillation MAC, vous pouvez configurer l'option tap-mode sur l'ensemble en ligne. Cependant, si le Firewall Threat Defense à haute disponibilité est configuré, vous devez activer l'apprentissage MAC pour la gestion des connexions lors d'un basculement. Ainsi, dans un environnement ACI avec Firewall Threat Defense dans une paire à haute disponibilité utilisant des interfaces d'ensemble en ligne, pour éviter les pertes de paquet, déployez Firewall Threat Defense en mode autonome ou dans une grappe.

Paramètres par défaut du mode de contexte multiple

- Par défaut, l'ASA est en mode de contexte unique.
- Consultez Classe par défaut, à la page 9.

Configurer plusieurs contextes

Procédure

Étape 1 Activer ou désactiver le mode de contexte multiple, à la page 16.

Étape 2 (Facultatif) Configurer une classe pour la gestion des ressources, à la page 18

Remarque
Pour la prise en charge VPN, vous devez configurer des ressources VPN dans une classe de ressources; la classe par défaut n'autorise pas le VPN.

Étape 3 Configurez les interfaces dans l'espace d'exécution du système.

- Firepower 1100, Firepower 2100 en mode Appliance (appareil), Secure Firewall 3100 -Configuration de l'interface de base.
- Firepower 2100 en mode plateforme : consultez le guide de démarrage.
- Firepower 4100/9300—Périphériques logiques pour le Firepower 4100/9300

Étape 4 Configurer un contexte de sécurité, à la page 22.

Étape 5 (Facultatif) Attribuer automatiquement des adresses MAC aux interfaces de contexte, à la page 26

Étape 6 Terminez la configuration de l'interface dans le contexte. Consultez Interfaces en mode routage et en mode transparent.

Activer ou désactiver le mode de contexte multiple

Votre ASA est peut-être déjà configuré pour plusieurs contextes de sécurité selon la façon dont vous l'avez commandé auprès de Cisco. Si vous devez passer du mode unique au mode multiple, suivez les procédures de cette section.

Activer le mode de contexte multiple

Lorsque vous passez du mode unique au mode multiple, l'ASA convertit la configuration d'exécution en deux fichiers : une nouvelle configuration de démarrage qui comprend la configuration système et admin.cfg qui comprend le contexte d'administration (dans le répertoire racine de la mémoire flash interne). La configuration d'exécution d'origine est enregistrée sous le nom old_running.cfg (dans le répertoire racine de la mémoire flash interne). La configuration de démarrage d'origine n'est pas enregistrée. L'ASA ajoute automatiquement une entrée pour le contexte d'administration à la configuration système avec le nom « administration ».

Avant de commencer

Sauvegardez votre configuration de démarrage si elle diffère de la configuration d'exécution. Lorsque vous passez du mode unique au mode multiple, l'ASA convertit la configuration d'exécution en deux fichiers. La configuration de démarrage d'origine n'est pas enregistrée. Voir Sauvegarde et restauration de configurations ou d'autres fichiers.

Procédure

Passez en mode de contexte multiple.

mode multiple

Exemple :

Vous êtes invité à changer de mode et à convertir la configuration, puis le système se recharge.

Remarque
Vous devrez régénérer la paire de clés RSA dans le contexte d'administration avant de pouvoir rétablir une connexion SSH. Dans la console, saisissez la commande **crypto key generate rsa modulus**. Consultez Configurer l'accès SSH pour de plus amples renseignements.

Exemple :

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#


***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system



***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

Rétablir le mode de contexte unique

Pour copier l'ancienne configuration en cours d'exécution dans la configuration de démarrage et changer le mode en mode unique, procédez comme suit.

Avant de commencer

Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Copiez la version de sauvegarde de votre configuration d'origine en cours d'exécution dans la configuration de démarrage actuelle :

copy disk0:old_running.cfg startup-config

Exemple :

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

Étape 2 Définissez le mode en mode unique :

mode unique

Exemple :

```
ciscoasa(config)# mode single
```

Vous êtes invité à redémarrer l'ASA.

Configurer une classe pour la gestion des ressources

Pour configurer une classe dans la configuration système, procédez comme suit. Vous pouvez modifier la valeur d'une limite de ressource particulière en entrant la commande avec une nouvelle valeur.

Avant de commencer

- Exécutez cette procédure dans l'espace d'exécution du système.
- Le tableau suivant répertorie les types de ressources et leurs limites. Consultez également la commande **show resource types**.

Remarque Si la limite du système est S.O., vous ne pouvez pas définir de pourcentage de la ressource, car il n'y a pas de limite de système stricte pour la ressource.

Tableau 1 : Noms et limites des ressources

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
asdm	Simultané	Au moins 1 5 au maximum	200	Sessions de gestion ASDM Les sessions ASDM utilisent deux connexions HTTPS: une pour la surveillance qui est toujours présente et une pour apporter des modifications de configuration qui est présente uniquement lorsque vous apportez des modifications. Par exemple, la limite système de 200 sessions ASDM représente une limite de 400 sessions HTTPS.

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
Connex.	Simultané ou taux	S. O.	Connexions simultanées : consultez Licences par modèle pour connaître la limite de connexions disponibles correspondant à votre modèle. Taux : S.O.	Connexions TCP ou UDP entre deux hôtes, y compris les connexions entre un hôte et plusieurs autres hôtes. **Remarque** Des messages syslog sont générés pour la limite la plus basse, xlates ou conns. Par exemple, si vous définissez la limite de xlates à 7 et le conns à 9, alors l'ASA génère uniquement le message syslog 321001 (« Resource xlates » limite de 7 atteinte pour le contexte « ctx1 ») et non 321002 (« Resource « conn rate » limite de 5 atteinte pour le contexte « ctx1 »).
hôtes	Simultané	s.o.	s.o.	Les hôtes pouvant se connecter par l'intermédiaire de l'ASA.
Inspections	Taux	s.o.	s.o.	nombre d'inspections d'applications par seconde
mac-addresses	Simultané	S. O.	(varie selon le modèle)	Pour le mode de pare-feu transparent, le nombre d'adresses MAC autorisées dans le tableau d'adresses MAC.
routes	Simultané	s.o.	s.o.	routes dynamiques.
vpn burst anyconnect	Simultané	S. O.	Les homologues premium Secure Client (services client sécurisés) correspondant à votre modèle moins la somme des sessions attribuées à tous les contextes pour **vpn anyconnect**.	Le nombre de sessions Secure Client (services client sécurisés) autorisées au-delà de la quantité attribuée à un contexte avec **vpn anyconnect**. Par exemple, si votre modèle prend en charge 5 000 homologues et que vous affectez 4 000 homologues dans tous les contextes avec **vpn anyconnect**, les 1 000 sessions restantes sont disponibles pour **vpn burst anyconnect**. Contrairement à **vpn anyconnect**, qui garantit les sessions au contexte, le **vpn burst anyconnect** peut être surabonné; le groupement de rafales est disponible pour tous les contextes selon le principe du premier arrivé, premier servi.

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
vpn anyconnect	Simultané	S. O.	Consultez Licences par modèle pour connaître les homologues Premium Secure Client (services client sécurisés) disponibles correspondant à votre modèle.	Homologues Secure Client (services client sécurisés). Vous ne pouvez pas surabonner cette ressource; toutes les affectations de contexte combinées ne peuvent pas dépasser la limite du modèle. Les homologues que vous affectez pour cette ressource sont garantis par le contexte.
vpn burst other	Simultané	S. O.	Le nombre de sessions Autre VPN correspondant à votre modèle moins la somme des sessions assignées à tous les contextes pour **vpn other**.	Le nombre de sessions VPN de site à site autorisées au-delà de la quantité attribuée à un contexte avec l'option **vpn other**. Par exemple, si votre modèle prend en charge 5 000 homologues et que vous affectez 4 000 homologues dans tous les contextes avec **vpn anyconnect**, les 1 000 sessions restantes sont disponibles pour **vpn burst anyconnect**. Contrairement à **vpn other**, qui garantit les sessions au contexte, **vpn burst other** peut être sursouscrit ; le groupement de rafales est disponible pour tous les contextes sur la base du premier arrivé, premier servi.
vpn other	Simultané	S. O.	Consultez Licences de fonctionnalités prises en charge par modèle pour connaître les autres sessions VPN disponibles correspondant à votre modèle.	Sessions VPN de site à site. Vous ne pouvez pas surabonner cette ressource; toutes les affectations de contexte combinées ne peuvent pas dépasser la limite du modèle. Les sessions que vous affectez pour cette ressource sont garanties par le contexte.
ikEv1 en négociation	Simultané (pourcentage uniquement)	S. O.	Un pourcentage des autres sessions VPN attribuée à ce contexte. Consultez les ressources **vpn other** pour attribuer des sessions au contexte.	Négociations IKEv1 SA entrantes, en tant que pourcentage de la limite du contexte de l'autre VPN.
ssh	Simultané	Au moins 1 5 au maximum	100	Séances SSH.

Nom de la ressource	Taux ou simultané	Nombre minimal et maximal par contexte	Limite du système	Description
stockage	Mo	Le maximum dépend du lecteur de mémoire flash que vous avez spécifié	Le maximum dépend du lecteur de mémoire flash que vous avez spécifié	Limite de stockage du répertoire de contexte en Mo. Spécifiez le lecteur à l'aide de la commande **storage-url**.
syslogs	Taux	s.o.	s.o.	Messages syslog par seconde.
telnet	Simultané	Au moins 1 5 au maximum	100	Sessions Telnet.
xlates	Simultané	s.o.	s.o.	Traduction d'adresses de réseau.

Procédure

Étape 1 Précisez le nom de la classe et accédez au mode de configuration de celle-ci :

class *name*

Exemple :

```
ciscoasa(config)# class gold
```

Le *name* (nom) est une chaîne de 20 caractères maximum. Pour définir les limites de la classe par défaut, saisissez « **default** » pour le nom.

Étape 2 Définir la limite de ressource pour un type de ressource :

limit-resource [**rate**] *resource_name number*[**%**]

Exemple :

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- Consultez le tableau précédent pour une liste des types de ressources. Si vous spécifiez **all**, toutes les ressources sont configurées avec la même valeur. Si vous spécifiez également une valeur pour une ressource particulière, la limite remplace la limite définie pour **all**.
- Saisissez l'argument **rate** pour définir le débit par seconde pour certaines ressources.
- Pour la plupart des ressources, spécifiez **0** comme *nombre* pour définir la ressource comme illimitée ou comme limite du système, le cas échéant. Pour les ressources VPN, la valeur **0** définit la limite à Aucun.
- Pour les ressources qui n'ont pas de limite système, vous ne pouvez pas définir le pourcentage (**%**). vous ne pouvez définir qu'une valeur absolue.

- Si vous définissez également la commande **quota management-session** dans un contexte pour définir le nombre maximal de sessions administratives (SSH, etc.), la valeur la plus basse sera utilisée.

Exemple

Par exemple, pour définir la limite de classe par défaut pour les connexions à 10 % au lieu d'illimité et pour autoriser 5 tunnels VPN de site à site avec 2 tunnels pour la rafale VPN, saisissez les commandes suivantes :

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

Toutes les autres ressources restent à illimité.

Pour ajouter une classe appelée gold, utilisez les commandes suivantes :

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

Lorsqu'un contexte est configuré avec une classe de ressources, une vérification est effectuée. Un avertissement est généré si les licences appropriées n'ont pas été installées avant les tentatives de connexion d'accès à distance VPN. L'administrateur doit ensuite obtenir une licence Secure Client Premier. Par exemple, un avertissement comme le suivant peut s'afficher :

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn anyconnect 10.0%
ciscoasa(config-class)# context test
Creating context 'text'...Done. (3)
ciscoasa(config-ctx)# member vpn
WARNING: Multi-mode remote access VPN support requires an AnyConnect Apex license.
Warning: An Access Context license is required for remote-access VPN support in multi-mode.
ciscoasa(config-ctx)#
```

Configurer un contexte de sécurité

La définition du contexte de sécurité dans la configuration système identifie le nom du contexte, l'URL du fichier de configuration, les interfaces qu'un contexte peut utiliser et d'autres paramètres.

Avant de commencer

- Exécutez cette procédure dans l'espace d'exécution du système.
- Configurer les interfaces. Pour les contextes en mode transparent, vous ne pouvez pas partager des interfaces entre les contextes, vous pouvez donc utiliser des sous-interfaces. Pour planifier l'utilisation de l'interface de gestion, consultez Utilisation de l'interface de gestion, à la page 8.
  - Firepower 1100, Firepower 2100 en mode Appliance (appareil), Secure Firewall 3100 -Configuration de l'interface de base.
  - Firepower 2100 en mode plateforme : consultez le guide de démarrage.
  - Firepower 4100/9300—Périphériques logiques pour le Firepower 4100/9300
- Si vous n'avez pas de contexte d'administration (par exemple, si vous effacez la configuration), vous devez d'abord préciser le nom du contexte d'administration en saisissant la commande suivante :

```
ciscoasa(config)# admin-context name
```

Bien que ce contexte n'existe pas encore dans votre configuration, vous pouvez par la suite entrer la commande « **context** *Name* » pour poursuivre la configuration du contexte d'administration.

Procédure

Étape 1 Ajouter ou modifier un contexte :

context *name*

Exemple :

```
ciscoasa(config)# context admin
```

Le *name* (nom) est une chaîne de 32 caractères maximum. Ce nom est sensible à la casse, vous pouvez donc avoir deux contextes nommés « clientA » et « ClientA », par exemple. Vous pouvez utiliser des lettres, des chiffres ou des tirets, mais vous ne pouvez pas commencer ou terminer le nom par un tiret.

Remarque
« System » ou « Null » (en lettres majuscules ou minuscules) sont des noms réservés et ne peuvent pas être utilisés.

Étape 2 (Facultatif) Ajoutez une description pour ce contexte :

description *texte*

Exemple :

```
ciscoasa(config-ctx)# description Admin Context
```

Étape 3 Précisez les interfaces que vous pouvez utiliser dans le contexte :

Pour allouer une interface :

allocate-interface *interface_id* [*mapped_name*] [**visible** | **invisible**]

Pour allouer une ou plusieurs sous-interfaces :

allocate-interface *interface_id.subinterface* [**-***interface_id.subinterface*] [*mapped_name*[**-***mapped_name*]] [**visible** | **invisible**]

Exemple :

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

Remarque
N'incluez pas d'espace entre le type d'interface et le numéro de port.

- Saisissez ces commandes plusieurs fois pour spécifier différentes plages. Si vous supprimez une allocation avec la forme **no** de cette commande, toutes les commandes de contexte qui incluent cette interface sont supprimées de la configuration en cours.
- Vous pouvez affecter les mêmes interfaces à plusieurs contextes en mode routé, si vous le souhaitez. Le mode transparent n'autorise pas les interfaces partagées.
- Le *mappé_name* (nom mapppé) est un alias alphanumérique pour l'interface qui peut être utilisé dans le contexte au lieu de l'ID de l'interface. Si vous ne spécifiez pas de nom mappé, l'ID d'interface est utilisé dans le contexte. Pour des raisons de sécurité, vous pouvez ne pas vouloir que l'administrateur de contexte sache quelles interfaces le contexte utilise. Un nom mappé doit commencer par une lettre, se terminer par une lettre ou un chiffre et avoir comme caractères internes uniquement des lettres, des chiffres ou un trait de soulignement. Par exemple, vous pouvez utiliser les noms suivants : **int0**, **inta**, **int_0**.
- Si vous spécifiez une plage de sous-interfaces, vous pouvez spécifier une plage correspondante de noms mappés. Suivez les directives suivantes concernant les plages :
  - Le nom mappé doit comprendre une partie alphabétique suivie d'une partie numérique. La partie alphabétique du nom mappé doit correspondre aux deux extrémités de la plage. Par exemple, saisissez la plage suivante : **int0-int10**. Si vous saisissez gig0/1.1-gig0/1.5 **happy**1-**sad**5, par exemple, la commande échoue.
  - La partie numérique du nom mappé doit inclure le même nombre de chiffres que la plage de la sous-interface. Par exemple, les deux plages comprennent 100 interfaces :**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100**. Si vous saisissez gig0/0.**100**-gig0/0.**199** int**1**-int**15**, par exemple, la commande échoue.
- Précisez **visible** pour voir le véritable ID de l'interface dans la commande **show interface** si vous définissez un nom mappé. Le mot clé par défaut **invisible** affiche uniquement le nom mappé.

Étape 4 Déterminez l'URL à partir de laquelle le système télécharge la configuration de contexte :

config-url *url*

Vous pouvez spécifier un fichier dans la mémoire flash ou sur un serveur distant.

Exemple :

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

Étape 5 (Facultatif) Autoriser chaque contexte à utiliser la mémoire flash pour stocker les paquets VPN, tels que Secure Client (services client sécurisés), ainsi que fournir le stockage pour Secure Client (services client sécurisés) SSL VPN sans client. Par exemple, si vous utilisez le mode de contexte multiple pour configurer un profil Secure Client (services client sécurisés) avec des politiques d'accès dynamique, vous devez planifier le stockage privé spécifique au contexte. Chaque contexte peut utiliser un espace de stockage privé ainsi qu'un espace de stockage partagé en lecture seule. **Remarque :** Assurez-vous que le répertoire cible est déjà présent sur le disque spécifié à l'aide de la commande **mkdir**.

storage-url {**private** | **shared**} [**disk***n***:/**]*path* [*context_label*]

Exemple :

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

Vous pouvez spécifier un espace de stockage **private** par contexte. Vous pouvez lire/écrire/supprimer à partir de ce répertoire dans le contexte (ainsi qu'à partir de l'espace d'exécution du système). Si vous ne spécifiez pas de numéro de disque, la valeur par défaut est disk0. Sous le *chemin* spécifié, ASA crée un sous-répertoire du nom du contexte. Par exemple, pour contexteA, si vous spécifiez **disk1:/private-storage** comme chemin, ASA crée un sous-répertoire pour ce contexte dans **disk1:/private-storage/contextA/**. Vous pouvez également éventuellement nommer le chemin dans le contexte avec une *context_label*, afin que le système de fichiers ne soit pas accessible aux administrateurs de contexte. Par exemple, si vous définissez la propriété *context_label* comme**context**, dans le contexte, ce répertoire s'appelle **context:**. Pour contrôler la quantité d'espace disque autorisée par contexte, consultez Configurer une classe pour la gestion des ressources, à la page 18.

Vous pouvez spécifier un espace de stockage **shared** en lecture seule par contexte, mais vous pouvez créer plusieurs répertoires partagés. Pour réduire la duplication de fichiers volumineux communs qui peuvent être partagés dans tous les contextes, tels que les paquets Secure Client (services client sécurisés), vous pouvez utiliser l'espace de stockage partagé. L'ASA ne crée pas de sous-répertoires de contexte pour cet espace de stockage, car il s'agit d'un espace partagé par plusieurs contextes. Seul l'espace d'exécution du système peut écrire et supprimer dans le répertoire partagé.

Étape 6 (Facultatif) Attribuez le contexte à une classe de ressources :

member *class_name*

Exemple :

```
ciscoasa(config-ctx)# member gold
```

Si vous ne spécifiez aucune classe, le contexte appartient à la classe par défaut. Vous ne pouvez affecter un contexte qu'à une seule classe de ressources.

Étape 7 (Facultatif) Attribuez un contexte à un groupe de basculement dans Basculement actif/Actif :

join-failover-group {**1** | **2**}

Exemple :

```
ciscoasa(config-ctx)# join-failover-group 2
```

Par défaut, les contextes sont dans le groupe 1. Le contexte d'administration doit toujours être dans le groupe 1.

Étape 8 (Facultatif) Activer Cloud Web Security pour ce contexte :

scansafe [**license** *key*]

Exemple :

```
ciscoasa(config-ctx)# scansafe
```

Si vous ne spécifiez pas de **license**, le contexte utilise la licence configurée dans la configuration système. L'ASA envoie la clé d'authentification aux serveurs mandataires de Cloud Web Security pour indiquer de quelle organisation provient la demande. La clé d'authentification est un nombre hexadécimal de 16 octets.

Consultez le guide de configuration du pare-feu pour obtenir des renseignements détaillés sur ScanSafe.

Exemple

L'exemple suivant définit le contexte d'administration sur « administrator », crée un contexte appelé « administrator » sur la mémoire flash interne, puis ajoute deux contextes d'un serveur FTP :

```
ciscoasa(config)# admin-context admin
ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

Attribuer automatiquement des adresses MAC aux interfaces de contexte

Cette section décrit comment configurer la génération automatique des adresses MAC. L'adresse MAC est utilisée pour classer les paquets dans un contexte.

Avant de commencer

- Lorsque vous configurez un de commande **« nameif »** pour l'interface dans un contexte, la nouvelle adresse MAC est générée immédiatement. Si vous activez cette fonctionnalité après avoir configuré les interfaces de contexte, les adresses MAC sont générées pour toutes les interfaces immédiatement après leur activation. Si vous désactivez cette fonctionnalité, l'adresse MAC par défaut de chaque interface

revient à l'adresse MAC. Par exemple, les sous-interfaces de GigabitEthernet 0/1 utilisent l'adresse MAC de GigabitEthernet 0/1.

- Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC de l'interface dans le contexte.

Procédure

Attribuez automatiquement des adresses MAC privées à chaque interface de contexte :

mac-address auto [**prefix** *prefix*]

Exemple :

```
ciscoasa(config)# mac-address auto prefix 19
```

Si vous n'écrivez pas de préfixe, l'ASA génère automatiquement ce dernier en fonction des deux derniers octets de l'.

Si vous saisissez manuellement un préfixe, le *préfixe* est une valeur décimale comprise entre 0 et 65 535. Ce préfixe est converti en nombre hexadécimal à quatre chiffres et utilisé dans l'adresse MAC.

Changer entre les contextes et l'espace d'exécution du système

Si vous vous connectez à l'espace d'exécution du système (ou au contexte d'administration), vous pouvez passer d'un contexte à l'autre et effectuer des tâches de configuration et de surveillance dans chaque contexte. La configuration en cours d'exécution que vous modifiez en mode de configuration ou qui est utilisée dans les commandes **de copie** ou **d'écriture** dépend de votre emplacement. Lorsque vous êtes dans l'espace d'exécution du système, la configuration en cours d'exécution se compose uniquement de la configuration système; lorsque vous êtes dans un contexte, la configuration en cours d'exécution comprend uniquement ce contexte. Par exemple, vous ne pouvez pas afficher toutes les configurations en cours d'exécution (système plus tous les contextes) en saisissant la commande **show running-config**. Seule la configuration actuelle s'affiche.

Procédure

Étape 1 Passez à un contexte :

changeto context *name*

L'invite passe à ciscoasa/*name*#

Étape 2 Passez à l'espace d'exécution du système :

changeto system

L'invite passe à ciscoasa#

Gérer les contextes de sécurité

Cette section décrit comment gérer les contextes de sécurité.

Supprimer un contexte de sécurité

Vous ne pouvez pas supprimer le contexte d'administration actuel, sauf si vous supprimez tous les contextes à l'aide de la commande **clear context**.

Remarque Si vous utilisez le basculement, il y a un délai entre le moment où vous supprimez le contexte sur l'unité active et le moment où le contexte est supprimé de l'unité en veille. Vous pourriez voir un message d'erreur indiquant que le nombre d'interfaces sur les unités actives et en veille n'est pas cohérent; cette erreur est temporaire et peut être ignorée.

Avant de commencer

Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Supprimez un seul contexte :

no context *name*

Toutes les commandes de contexte sont également supprimées. Le fichier de configuration de contexte n'est pas supprimé de l'emplacement de l'URL de configuration.

Étape 2 Supprimez tous les contextes (y compris le contexte d'administration) :

clear context

Les fichiers de configuration de contexte ne sont pas supprimés des emplacements des URL de configuration.

Modifier le contexte d'administration

La configuration système n'inclut aucune interface réseau ni aucun paramètre réseau pour elle-même; au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise l'un des contextes désigné comme contexte d'administration.

Le contexte d'administration est similaire à tout autre contexte, sauf que lorsqu'un utilisateur se connecte au contexte d'administration, cet utilisateur dispose de droits d'administrateur système et peut accéder au système et à tous les autres contextes. Le contexte admin n'est limité en aucune façon et peut être utilisé comme contexte standard. Cependant, comme la connexion au contexte admin vous accorde des privilèges d'administrateur sur tous les contextes, vous devrez peut-être restreindre l'accès au contexte admin aux utilisateurs appropriés.

Avant de commencer

- Vous pouvez définir n'importe quel contexte comme contexte d'administration, tant que le fichier de configuration est stocké dans la mémoire flash interne.
- Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Définissez le contexte d'administration :

admin-context *context_name*

Exemple :

```
ciscoasa(config)# admin-context administrator
```

Toutes les sessions de gestion à distance, telles que Telnet, SSH ou HTTPS, qui sont connectées au contexte d'administration sont terminées. Vous devez vous reconnecter au nouveau contexte d'administration.

Quelques commandes de configuration système, notamment **ntp server**, identifient un nom d'interface qui appartient au contexte d'administration. Si vous modifiez le contexte d'administration et que le nom de l'interface n'existe pas dans le nouveau contexte d'administration, veillez à mettre à jour toutes les commandes système qui font référence à l'interface.

Modifier l'URL du contexte de sécurité

Cette section décrit comment modifier l'URL du contexte.

Avant de commencer

- Vous ne pouvez pas modifier l'URL du contexte de sécurité sans recharger la configuration à partir de la nouvelle URL. L'ASA fusionne la nouvelle configuration avec la configuration en cours d'exécution.
- La saisie de la même URL fusionne également la configuration enregistrée avec la configuration d'exécution.
- Une fusion ajoute toutes les nouvelles commandes de la nouvelle configuration à la configuration en cours d'exécution.
  - Si les configurations sont identiques, aucune modification ne se produit.
  - Si des commandes sont en conflit ou si des commandes influent sur le fonctionnement du contexte, l'effet de la fusion dépend de la commande. Vous pourriez obtenir des erreurs ou des résultats inattendus. Si la configuration d'exécution est vide (par exemple, si le serveur n'est pas disponible et que la configuration n'a jamais été téléchargée), la nouvelle configuration est utilisée.
- Si vous ne souhaitez pas fusionner les configurations, vous pouvez effacer la configuration d'exécution, ce qui perturbe toute communication en raison du contexte, puis recharger la configuration à partir de la nouvelle URL.

- Exécutez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 (Facultatif, si vous ne souhaitez pas effectuer de fusion) Modifiez le contexte et effacez la configuration :

changeto context *name*

clear configure all

Exemple :

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(config)# clear configure all
```

Si vous souhaitez effectuer une fusion, passez à l'étape 2.

Étape 2 Passez à l'espace d'exécution du système :

changeto system

Exemple :

```
ciscoasa/ctx1(config)# changeto system
ciscoasa(config)#
```

Étape 3 Entrez en mode de configuration du contexte pour le contexte que vous souhaitez modifier.

context *name*

Exemple :

```
ciscoasa(config)# context ctx1
```

Étape 4 Saisissez la nouvelle URL. Le système charge immédiatement le contexte pour qu'il s'exécute.

config-url *new_url*

Exemple :

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

Recharger un contexte de sécurité

Vous pouvez recharger le contexte de deux manières :

- Effacez la configuration en cours d'exécution, puis importez la configuration de démarrage.

  Cette action efface la plupart des attributs associés au contexte, tels que les connexions et les tables NAT.
- Supprimez le contexte de la configuration système.

Cette action efface les attributs supplémentaires, tels que l'allocation de mémoire, qui pourraient être utiles pour le dépannage. Cependant, pour rajouter le contexte au système, vous devez redéfinir l'URL et les interfaces.

Recharger en effaçant la configuration

Procédure

Étape 1 Passez au contexte que vous souhaitez recharger :

changeto context *name*

Exemple :

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(comfig)#
```

Étape 2 Effacez la configuration d'exécution :

clear configure all

Cette commande efface toutes les connexions.

Étape 3 Rechargez la configuration :

copy startup-config running-config

Exemple :

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

L'ASA copie la configuration à partir de l'URL spécifiée dans la configuration système. Vous ne pouvez pas modifier l'URL à partir d'un contexte.

Recharger en supprimant et en rajoutant le contexte

Pour recharger le contexte en le supprimant, puis en le rajoutant, procédez comme suit.

Procédure

Étape 1 Supprimer un contexte de sécurité, à la page 28. **Also delete config URL file from the disk**

Étape 2 Configurer un contexte de sécurité, à la page 22

Supervision des contextes de sécurité

Cette section décrit comment afficher et superviser les renseignements contextuels.

Afficher les informations de contexte

À partir de l'espace d'exécution du système, vous pouvez afficher une liste de contextes, y compris le nom, les interfaces allouées et l'URL du fichier de configuration.

Procédure

Affichez tous les contextes :

show context [*name* | **detail**| **count**]

Si vous souhaitez afficher des renseignements pour un contexte particulier, spécifiez le *nom*.

L'option **detail** (détail) affiche des renseignements supplémentaires. Consultez les exemples de sortie ci-dessous suivants pour en savoir plus.

L'option **count** (nombre) affiche le nombre total de contextes.

Exemple

Voici un exemple de sortie de la commande **show context** . L'exemple de sortie suivant montre trois contextes :

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

Le tableau suivant affiche la description de chaque champ.

Tableau 2 : afficher les champs de contexte

Champ	Description
Nom du contexte	Répertorie tous les noms de contexte. Le nom du contexte avec l'astérisque (*) est le contexte d'administration.
Interfaces	Les interfaces attribuées au contexte.

Champ	Description
URL	L'URL à partir de laquelle l'ASA charge la configuration de contexte.

Voici un exemple de sortie de la commande **show context detail** :

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

Consultez la référence de commande pour en savoir plus sur la sortie **detail** (détail).

Voici un exemple de sortie de la commande **show context count** :

```
ciscoasa# show context count
Total active contexts: 2
```

Afficher l'affectation des ressources

À partir de l'espace d'exécution du système, vous pouvez afficher l'allocation pour chaque ressource pour toutes les classes et les membres de classe.

Procédure

Affichez l'allocation des ressources :

show resource allocation [**detail**]

Cette commande affiche l'allocation de ressources, mais n'affiche pas les ressources réelles utilisées. Consultez Afficher l'utilisation des ressources, à la page 36 pour de plus amples renseignements sur l'utilisation réelle des ressources.

L'argument **detail** affiche des renseignements supplémentaires. Consultez les exemples de sortie suivants pour en savoir plus.

Exemple

L'exemple de sortie suivant affiche l'allocation totale de chaque ressource en valeur absolue et en pourcentage des ressources système disponibles :

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Routes                      5000           N/A
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 AnyConnect                  1000           10%
 AnyConnectBurst              200           2%
 Other VPN Sessions            20           2.66%
 Other VPN Burst               20           2.66%
 All                    unlimited
```

Le tableau suivant affiche la description de chaque champ.

Tableau 3 : afficher les champs d'allocation de ressources

Champ	Description
Resource (Ressource)	Le nom de la ressource que vous pouvez limiter.
Total	La quantité totale de ressources allouées à tous les contextes. La quantité est un nombre absolu d'instances ou d'instances simultanées par seconde. Si vous avez spécifié un pourcentage dans la définition de la classe, l'ASA convertit le pourcentage en un nombre absolu pour cet affichage.
% of Avail (% de disponibilité)	Le pourcentage des ressources système totales allouées pour tous les contextes, si la ressource a une limite de système matériel. Si une ressource n'a pas de limite de système, cette colonne indique S.O.

L'exemple suivant illustre la sortie de la commande **show resource allocation detail** :

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
```

```
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Telnet           default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Routes           default          all       C  unlimited                N/A
                 gold               1       D  unlimited          5      N/A
                 silver             1      CA         10         10      N/A
                 bronze             0      CA          5                 N/A
                 All Contexts:      3                            20      N/A

Xlates           default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      23040      23040     N/A
                 bronze             0      CA      11520
                 All Contexts:      3                         23040     N/A

mac-addresses    default          all       C      65535
                 gold               1       D      65535      65535    100.00%
                 silver             1      CA       6553       6553      9.99%
                 bronze             0      CA       3276
                 All Contexts:      3                        137623    209.99%
```

Le tableau suivant affiche la description de chaque champ.

Tableau 4 : afficher les champs de détail de l'allocation des ressources

Champ	Description
Resource (Ressource)	Le nom de la ressource que vous pouvez limiter.
Classe	Le nom de chaque classe, y compris la classe par défaut. Le champ All contexts (Tous les contextes) affiche les valeurs totales pour toutes les classes.
Mmbrs (Membres)	Le nombre de contextes affectés à chaque classe.
Origin (Origine)	L'origine de la limite de ressources, comme suit : • R : vous définissez cette limite avec l'option **all** (toutes), plutôt qu'en tant que ressource individuelle. • C : cette limite est issue de la classe de membres. • D : cette limite n'a pas été définie dans la classe de membres, mais est issue de la classe par défaut. Pour un contexte attribué à la classe par défaut, la valeur sera « C » au lieu de « D ». L'ASA peut combiner « A » avec « C » ou « D ».
Limit (Limite)	La limite de la ressource par contexte, sous forme de nombre absolu. Si vous avez spécifié un pourcentage dans la définition de la classe, l'ASA convertit le pourcentage en un nombre absolu pour cet affichage.
Total	La quantité totale de ressources allouées à tous les contextes de la classe. La quantité est un nombre absolu d'instances ou d'instances simultanées par seconde. Si la ressource est illimitée, cet affichage est vide.
% of Avail (% de disponibilité)	Le pourcentage des ressources système totales allouées pour tous les contextes de la classe. Si la ressource est illimitée, cet affichage est vide. Si la ressource n'a pas de limite système, alors cette colonne indique S.O.

Afficher l'utilisation des ressources

À partir de l'espace d'exécution du système, vous pouvez afficher l'utilisation des ressources pour chaque contexte et afficher l'utilisation des ressources du système.

Procédure

Affichez l'utilisation des ressources pour chaque contexte :

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]

- Par défaut, **toute** l'utilisation des contextes est affichée; chaque contexte est répertorié séparément.

- Saisissez le mot clé **top** *n* pour afficher les contextes qui sont les *n* principaux utilisateurs de la ressource spécifiée. Vous devez spécifier un seul type de ressource, et non **toutes les ressources**, avec cette option.
- L'option **summary** affiche l'utilisation combinée de tous les contextes.
- L'option **system** affiche toutes les utilisations de contexte combinées, mais affiche les limites du système pour les ressources au lieu des limites de contexte combinées.
- Pour la **ressource** *resource_name*, consultez Configurer une classe pour la gestion des ressources, à la page 18 pour connaître les noms de ressources disponibles. Consultez également la commande **show resource type**. Spécifiez **tout** (par défaut) pour tous les types.
- L'option **detail** affiche l'utilisation de toutes les ressources, y compris celles que vous ne pouvez pas gérer. Par exemple, vous pouvez afficher le nombre d'interceptions TCP.
- Le **compteur** *counter_name* est l'un des mots clés suivants :
  - **current** : affiche les instances simultanées actives ou le débit actuel de la ressource.
  - **denied** : affiche le nombre d'instances qui ont été refusées parce qu'elles dépassaient la limite de ressources indiquée dans la colonne Limit (Limite).
  - **max** : affiche le nombre maximum d'instances simultanées ou le débit maximum de la ressource depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage** , soit en raison du redémarrage du périphérique.
  - **all** (par défaut) : affiche toutes les statistiques.
- Le *count_threshold* définit le nombre au-dessus duquel les ressources sont affichées. La valeur par défaut est 1. Si l'utilisation de la ressource est inférieure au nombre que vous avez défini, la ressource n'est pas affichée. Si vous spécifiez **all** pour le nom du compteur, le *count_threshold* s'applique à l'utilisation actuelle.
- Pour afficher toutes les ressources, définissez le *count_threshold* sur **0**.

Exemples

Voici un exemple de sortie de la commande **show resource usage context**, qui affiche l'utilisation des ressources pour le contexte d'administration :

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

Voici un exemple de sortie de la commande **show resource usage summary**, qui affiche l'utilisation des ressources pour tous les contextes et toutes les ressources. Cet exemple montre les limites de six contextes.

```
ciscoasa# show resource usage summary
```

```
Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      N/A            0 Summary
Conns                     584          763      280000(S)      0 Summary
Xlates                   8526         8966      N/A            0 Summary
Hosts                     254          254      N/A            0 Summary
Conns [rate]              270          535      N/A         1704 Summary
Inspects [rate]           270          535      N/A            0 Summary
AnyConnect                  2           25      1000           0 Summary
AnyConnectBurst             0            0      200            0 Summary
Other VPN Sessions          0           10      10           740 Summary
Other VPN Burst             0           10      10           730 Summary

S = System: Combined context limits exceed the system limit; the system limit is shown.
```

Voici un exemple de sortie de la commande **show resource usage summary**, qui affiche les limites pour 25 contextes. Étant donné que la limite de contexte pour les connexions Telnet et SSH est de 5 par contexte, la limite combinée est de 125. La limite du système n'étant que de 100, c'est cette limite qui est affichée.

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

Voici un exemple de sortie de la commande **show resource usage system**, qui affiche l'utilisation des ressources pour tous les contextes, mais qui indique la limite du système au lieu des limites combinées des contextes. L'option **counter all 0** est utilisée pour afficher les ressources qui ne sont pas utilisées actuellement. Les statistiques Denied indiquent le nombre de fois où la ressource a été refusée en raison de la limite du système, si disponible.

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit        Denied    Context
Telnet                      0            0        100             0    System
SSH                         0            0        100             0    System
ASDM                        0            0         32             0    System
Routes                      0            0        N/A             0    System
IPSec                       0            0          5             0    System
Syslogs [rate]              1           18        N/A             0    System
Conns                       0            1     280000             0    System
Xlates                      0            0        N/A             0    System
Hosts                       0            2        N/A             0    System
Conns [rate]                1            1        N/A             0    System
Inspects [rate]             0            0        N/A             0    System
AnyConnect                  2           25      10000             0    System
AnyConnectBurst             0            0        200             0    System
Other VPN Sessions          0           10        750           740    System
Other VPN Burst             0           10        750           730    System
```

Superviser les attaques SYN dans les contextes

L'ASA empêche les attaques SYN à l'aide de l'interception TCP. L'interception TCP utilise l'algorithme des témoins SYN pour empêcher les attaques par inondation TCP SYN. Une attaque par inondation SYN consiste en une série de paquets SYN provenant généralement d'adresses IP falsifiées. Le flux constant de paquets SYN maintient la file d'attente SYN du serveur pleine, ce qui l'empêche de répondre aux demandes de connexion. Lorsque le seuil de connexion amorce d'une connexion est franchi, l'ASA agit comme un serveur mandataire pour le serveur et génère une réponse SYN-ACK à la requête SYN du client. Lorsque l'ASA reçoit un ACK en retour du client, il peut alors authentifier le client et autoriser la connexion au serveur.

Procédure

Étape 1 Supervisez le taux d'attaques pour les contextes individuels :

show perfmon

Étape 2 Supervisez la quantité de ressources utilisées par l'interception TCP pour les contextes individuels :

show resource usage detail

Étape 3 Supervisez les ressources utilisées par l'interception TCP pour l'ensemble du système :

show resource usage summary detail

Exemples

Voici un exemple de sortie de la commande **show perfmon** qui affiche le taux d'interceptions TCP pour un contexte appelé admin.

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept    322779/s      322779/s
```

Voici un exemple de sortie de la commande **show resource usage detail** qui affiche la quantité de ressources utilisées par l'interception TCP pour les contextes individuels. (L'exemple de texte en **gras** affiche les renseignements d'interception TCP.)

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit        Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
chunk:static                1            1  unlimited             0 admin
tcp-intercepts         328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
statics                     1            1  unlimited             0 admin
ace-rules                   1            1  unlimited             0 admin
console-access-rul          2            2  unlimited             0 admin
fixup-rules                14           15  unlimited             0 admin
memory                 959872       960000  unlimited             0 c1
chunk:channels             15           16  unlimited             0 c1
chunk:dbgtrace              1            1  unlimited             0 c1
chunk:fixup                15           15  unlimited             0 c1
chunk:global                1            1  unlimited             0 c1
chunk:hole                  2            2  unlimited             0 c1
chunk:ip-users             10           10  unlimited             0 c1
chunk:udp-ctrl-blk          1            1  unlimited             0 c1
chunk:list-elem            24           24  unlimited             0 c1
chunk:list-hdr              5            6  unlimited             0 c1
chunk:nat                   1            1  unlimited             0 c1
chunk:route                 2            2  unlimited             0 c1
chunk:static                1            1  unlimited             0 c1
tcp-intercept-rate      16056        16254  unlimited             0 c1
globals                     1            1  unlimited             0 c1
np-statics                  3            3  unlimited             0 c1
statics                     1            1  unlimited             0 c1
nats                        1            1  unlimited             0 c1
ace-rules                   2            2  unlimited             0 c1
console-access-rul          2            2  unlimited             0 c1
fixup-rules                14           15  unlimited             0 c1
memory              232695716    232020648  unlimited             0 system
chunk:channels             17           20  unlimited             0 system
chunk:dbgtrace              3            3  unlimited             0 system
chunk:fixup                15           15  unlimited             0 system
chunk:ip-users              4            4  unlimited             0 system
chunk:list-elem          1014         1014  unlimited             0 system
chunk:list-hdr              1            1  unlimited             0 system
chunk:route                 1            1  unlimited             0 system
block:16384               510          885  unlimited             0 system
block:2048                 32           34  unlimited             0 system
```

L'exemple de sortie suivant affiche les ressources utilisées par l'interception TCP pour l'ensemble du système. (L'exemple de texte en **gras** affiche les renseignements d'interception TCP.)

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory              238421312    238434336  unlimited             0 Summary
chunk:channels             46           48  unlimited             0 Summary
chunk:dbgtrace              4            4  unlimited             0 Summary
chunk:fixup                45           45  unlimited             0 Summary
chunk:global                1            1  unlimited             0 Summary
chunk:hole                  3            3  unlimited             0 Summary
chunk:ip-users             24           24  unlimited             0 Summary
```

```
chunk:udp-ctrl-blk          1           1  unlimited            0 Summary
chunk:list-elem          1059        1059  unlimited            0 Summary
chunk:list-hdr             10          11  unlimited            0 Summary
chunk:nat                   1           1  unlimited            0 Summary
chunk:route                 5           5  unlimited            0 Summary
chunk:static                2           2  unlimited            0 Summary
block:16384               510         885  unlimited            0 Summary
block:2048                 32          35  unlimited            0 Summary
tcp-intercept-rate     341306      811579  unlimited            0 Summary
globals                     1           1  unlimited            0 Summary
np-statics                  6           6  unlimited            0 Summary
statics                     2           2        N/A            0 Summary
nats                        1           1        N/A            0 Summary
ace-rules                   3           3        N/A            0 Summary
console-access-rul          4           4        N/A            0 Summary
fixup-rules                43          44        N/A            0 Summary
```

Afficher les adresses MAC attribuées

Vous pouvez afficher les adresses MAC générées automatiquement dans la configuration système ou dans le contexte.

Afficher les adresses MAC dans la configuration système

Cette section décrit comment afficher les adresses MAC dans la configuration système.

Avant de commencer

Si vous attribuez manuellement une adresse MAC à une interface, mais que la génération automatique est également activée, l'adresse générée automatiquement continue de s'afficher dans la configuration même si l'adresse MAC manuelle est celle qui est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement s'affichera.

Procédure

Affichez les adresses MAC attribuées à partir de l'espace d'exécution du système :

show running-config all context [*name*]

L'option **all** (toutes) est requise pour afficher les adresses MAC attribuées. Bien que la commande **mac-address auto** puisse être configurée par l'utilisateur uniquement en mode de configuration globale, la commande s'affiche comme une entrée en lecture seule en mode de configuration du contexte avec l'adresse MAC attribuée. Seules les interfaces allouées qui sont configurées avec une commande **nameif** dans le contexte se voient attribuer une adresse MAC.

Exemples

La sortie suivante de la commande **show running-config all context admin** affiche les adresses MAC principale et de secours attribuées à l'interface de gestion Management0/0 :

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

La sortie suivante de la commande **show running-config all context** affiche toutes les adresses MAC (principales et de secours) pour toutes les interfaces de contexte. Notez que comme les interfaces principales GigabitEthernet0/0 et GigabitEthernet0/1 ne sont pas configurées avec la commande **nameif** dans les contextes, aucune adresse MAC n'a été générée pour elles.

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

Afficher les adresses MAC dans un contexte

Cette section décrit comment afficher les adresses MAC dans un contexte.

Procédure

Affichez l'adresse MAC utilisée par chaque interface dans le contexte :

show interface | include (Interface)|(MAC)

Exemple

Par exemple :

```
ciscoasa/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

Remarque La commande **show interface** affiche l'adresse MAC utilisée; si vous attribuez manuellement une adresse MAC et que la génération automatique est activée, vous ne pouvez afficher que l'adresse générée automatiquement inutilisée à partir de la configuration système.

Exemples de mode de contexte multiple

L'exemple suivant :

- Définit automatiquement les adresses MAC dans les contextes avec un préfixe personnalisé.
- Définit la limite de classe par défaut des connexions à 10 % au lieu d'un nombre illimité et définit le VPN pour les autres sessions à 10, avec une rafale de 5.
- Crée une classe de ressources Gold.
- Définit le contexte d'administration comme « administrateur ».
- Crée un contexte appelé « administrateur » sur la mémoire flash interne pour qu'il fasse partie de la classe de ressources par défaut.
- Ajoute deux contextes d'un serveur FTP dans le cadre de la classe de ressources Gold.

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 10
```

```
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50

ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

Historique du mode de contexte multiple

Tableau 5 : Historique du mode de contexte multiple

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Contextes de sécurité multiples	7.0(1)	Le mode de contexte multiple a été introduit. Nous avons introduit les commandes suivantes : **context**, **mode** et **class**.
Affectation automatique de l'adresse MAC	7.2(1)	L'affectation automatique de l'adresse MAC aux interfaces de contexte a été introduite. Nous avons introduit la commande suivante : **mac-address auto**.
Gestion des ressources	7.2(1)	La gestion des ressources a été introduite. Nous avons introduit les commandes suivantes : **class**, **limit-resource** et **member**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Capteurs virtuels pour IPS	8.0(2)	L'AIP SSM exécutant la version 6.0 et ultérieure du logiciel IPS peut exécuter plusieurs capteurs virtuels, ce qui signifie que vous pouvez configurer plusieurs politiques de sécurité sur l'AIP SSM. Vous pouvez affecter chaque contexte ou ASA en mode unique à un ou plusieurs capteurs virtuels, ou vous pouvez attribuer plusieurs contextes de sécurité au même capteur virtuel. Nous avons introduit la commande suivante : **allocate-ips**.
Améliorations de l'affectation automatique de l'adresse MAC	8.5(2)	Le format de l'adresse MAC a été modifié pour utiliser un préfixe, une valeur initiale fixe (A2) et un schéma différent pour les adresses MAC des unités principale et secondaire dans une paire de basculement. Les adresses MAC sont également conservées de façon permanente pendant les rechargements. L'analyseur de commande vérifie maintenant si la génération automatique est activée; si vous souhaitez également attribuer manuellement une adresse MAC, vous ne pouvez pas commencer l'adresse MAC manuelle par A2. Nous avons modifié la commande suivante : **mac-address auto prefix**.
Augmentation du nombre maximum de contextes pour les modèles ASA 5550 et 5580	v8.4(1)	Le nombre maximum de contextes de sécurité pour l'ASA 5550 est passé de 50 à 100. Le nombre maximum pour l'ASA 5580 est passé de 50 à 250.
Affectation automatique de l'adresse MAC activée par défaut	8.5(1)	L'affectation automatique de l'adresse MAC est maintenant activée par défaut. Nous avons modifié la commande suivante : **mac-address auto**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Génération automatique d'un préfixe d'adresse MAC	8.6(1)	En mode de contexte multiple, l'ASA convertit maintenant la configuration de génération automatique de l'adresse MAC en utilisant un préfixe par défaut. L'ASA génère automatiquement ce dernier en fonction des deux derniers octets de l'adresse MAC de l'interface (ASA 5500-X) ou du fond de panier (ASASM). Cette conversion se produit automatiquement lorsque vous rechargez ou si vous réactivez la génération d'adresse MAC. La méthode de génération du préfixe offre de nombreux avantages, notamment une meilleure garantie d'adresses MAC uniques sur un segment. Vous pouvez afficher le préfixe généré automatiquement en saisissant la commande **show running-config mac-address**. Si vous souhaitez modifier le préfixe, vous pouvez reconfigurer la fonctionnalité avec un préfixe personnalisé. L'ancienne méthode de génération d'adresse MAC n'est plus disponible. **Remarque** Pour maintenir la mise à niveau sans interruption pour les paires de basculement, l'ASA ne convertit *pas* la méthode de génération d'adresse MAC en une configuration existante lors d'un rechargement si le basculement est activé. Cependant, nous vous conseillons fortement de passer manuellement à la méthode de génération du préfixe lorsque vous utilisez le basculement, en particulier pour l'ASASM. Sans la méthode de préfixe, les ASASM installés dans différents numéros de logement subissent un changement d'adresse MAC lors du basculement et peuvent connaître une interruption du trafic. Après la mise à niveau, pour utiliser la méthode de préfixe de génération d'adresse MAC, réactivez la génération d'adresse MAC pour utiliser le préfixe par défaut. Nous avons modifié la commande suivante : **mac-address auto**.
Affectation automatique de l'adresse MAC désactivée par défaut sur tous les modèles à l'exception de l'ASASM	9.0(1)	L'affectation automatique de l'adresse MAC est maintenant désactivée par défaut, à l'exception de l'ASASM. Nous avons modifié la commande suivante : **mac-address auto**.
Routage dynamique dans les contextes de sécurité	9.0(1)	Les protocoles de routage dynamique EIGRP et OSPFv2 sont désormais pris en charge en mode de contexte multiple. Les routages OSPFv3, RIP et multidiffusion ne sont pas pris en charge.
Nouveau type de ressource pour les entrées de la table de routage	9.0(1)	Un nouveau type de ressource, les routes, a été créé pour définir le nombre maximum d'entrées de table de routage dans chaque contexte. Nous avons modifié les commandes suivantes : **limit-resource, show resource types, show resource usage, show resource allocation**.
VPN de site à site en mode de contexte multiple	9.0(1)	Les tunnels VPN de site à site sont désormais pris en charge en mode de contexte multiple.
Nouveau type de ressource pour les tunnels VPN de site à site	9.0(1)	De nouveaux types de ressources (vpn other et vpn burst other) ont été créés pour définir le nombre maximum de tunnels VPN de site à site dans chaque contexte. Nous avons modifié les commandes suivantes : **limit-resource, show resource types, show resource usage, show resource allocation**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Nouveau type de ressource pour les négociations de la SA IKEv1	9.1(2)	Un nouveau type de ressource (ikev1 in-negotiation) a été créé pour définir le pourcentage maximum de négociations de la SA IKEv1 dans chaque contexte afin d'éviter de submerger le CPU et les moteurs de chiffrement. Sous certaines conditions (certificats volumineux, vérification des CRL), vous souhaiterez peut-être restreindre cette ressource. Nous avons modifié les commandes suivantes : **limit-resource, show resource types, show resource usage, show resource allocation**.
Prise en charge du VPN d'accès à distance en mode de contexte multiple	9.5(2)	Vous pouvez désormais utiliser les fonctionnalités d'accès à distance suivantes en mode de contexte multiple : • AnyConnect 3.x ou versions ultérieures (SSL VPN uniquement; pas de prise en charge d'IKEv2) • Configuration centralisée de l'image Secure Client (services client sécurisés) • Mise à niveau de l'image Secure Client (services client sécurisés) • Gestion des ressources de contexte pour les connexions Secure Client (services client sécurisés) **Remarque** La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante. Nous avons introduit les commandes suivantes : **limit-resource vpn anyconnect, limit-resource vpn burst anyconnect**
Fonction de préremplissage/nom d'utilisateur à partir du certificat pour le mode de contexte multiple	9.6(2)	La prise en charge de SSL Secure Client (services client sécurisés) est étendue, ce qui permet aux interfaces de ligne de commande de la fonctionnalité de préremplissage/nom d'utilisateur à partir du certificat, qui étaient auparavant seulement disponibles en mode unique, d'être également activées en mode de contexte multiple. Nous n'avons pas modifié de commandes.
Virtualisation flash pour le VPN d'accès à distance	9.6(2)	Le VPN d'accès à distance en mode de contexte multiple prend désormais en charge la virtualisation flash. Chaque contexte peut avoir un espace de stockage privé et un emplacement de stockage partagé en fonction de la mémoire flash totale disponible : • Stockage privé : stockez les fichiers associés uniquement à cet utilisateur et spécifiques au contenu que vous souhaitez pour cet utilisateur. • Stockage partagé : chargez des fichiers dans cet espace et rendez-le accessible à n'importe quel contexte d'utilisateur pour un accès en lecture/écriture une fois que vous l'avez activé. Nous avons introduit les commandes suivantes : **limit-resource storage, storage-url**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Profils Secure Client (services client sécurisés) pris en charge dans les périphériques en contexte multiple	9.6(2)	Les profils Secure Client (services client sécurisés) sont pris en charge dans les périphériques en contexte multiple. Pour ajouter un nouveau profil à l'aide d'ASDM, vous devez disposer de la version Secure Client (services client sécurisés) 4.2.00748 ou 4.3.03013 et ultérieure.
Basculement avec état pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple	9.6(2)	Le basculement avec état est maintenant pris en charge pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple. Nous n'avons pas modifié de commandes.
La politique d'accès dynamique (DAP) du VPN d'accès à distance est prise en charge en mode de contexte multiple	9.6(2)	Vous pouvez maintenant configurer la DAP par contexte en mode de contexte multiple. Nous n'avons pas modifié de commandes.
Le CoA (changement d'autorisation) du VPN d'accès à distance est pris en charge en mode de contexte multiple	9.6(2)	Vous pouvez maintenant configurer le CoA par contexte en mode de contexte multiple. Nous n'avons pas modifié de commandes.
La localisation du VPN d'accès à distance est prise en charge en mode de contexte multiple	9.6(2)	La localisation est prise en charge dans le monde entier. Il n'y a qu'un seul ensemble de fichiers de localisation partagés dans différents contextes. Nous n'avons pas modifié de commandes.
Le VPN d'accès à distance pour IKEv2 est pris en charge en mode de contexte multiple	9.9(2)	Vous pouvez configurer le VPN d'accès à distance en mode de contexte multiple pour IKEv2.
Limitation configurable des sessions d'administration	9.12(1)	Vous pouvez configurer le nombre maximum de sessions administratives agrégées, par utilisateur et par protocole. Auparavant, vous pouviez configurer uniquement le nombre agrégé de sessions. Cette fonctionnalité n'influe pas sur les sessions de console. Notez qu'en mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions HTTPS, où le maximum est fixé à 5 sessions. La commande **quota management-session** n'est également plus acceptée dans la configuration système et est plutôt disponible dans la configuration du contexte. Le nombre maximum de sessions agrégées est désormais de 15; si vous avez configuré 0 (illimité) ou 16+, lors de la mise à niveau, la valeur passe à 15. Commandes nouvelles/modifiées : **quota management-session**, **show quota management-session**
Le nombre maximum de contextes de Firepower 1140 est passé de 5 à 10	9.16(1)	Le Firepower 1140 prend désormais en charge jusqu'à 10 contextes.

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.