

# Mode contexte multiple

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


- À propos des contextes de sécurité, à la page 1
- Licences pour le mode de contexte multiple, à la page 13
- Conditions préalables pour le mode de contexte multiple, à la page 14
- Lignes directrices pour le mode de contexte multiple, à la page 14
- Paramètres par défaut du mode de contexte multiple, à la page 15
- Configurer plusieurs contextes, à la page 15
- Changer entre les contextes et l'espace d'exécution du système, à la page 26
- Gérer les contextes de sécurité, à la page 26
- Supervision des contextes de sécurité, à la page 30
- Historique du mode de contexte multiple, à la page 33


# 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.

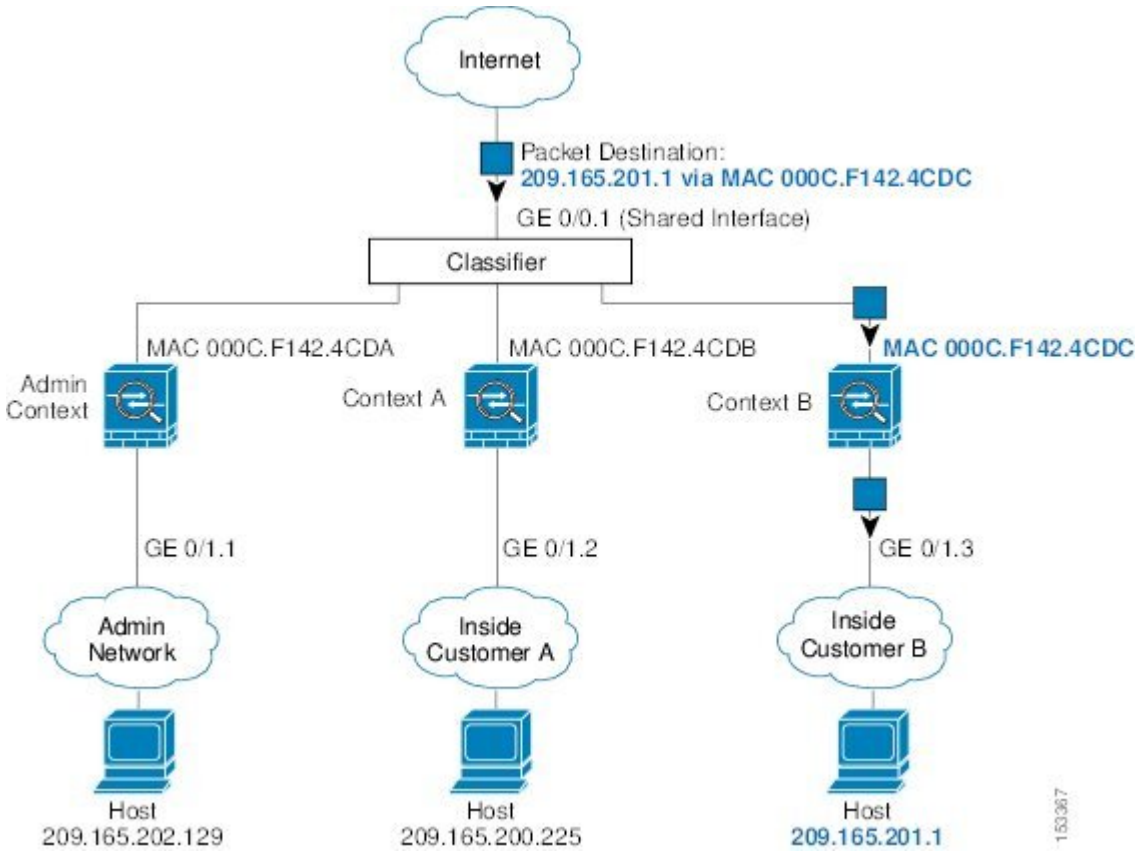
#### Configuration NAT

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

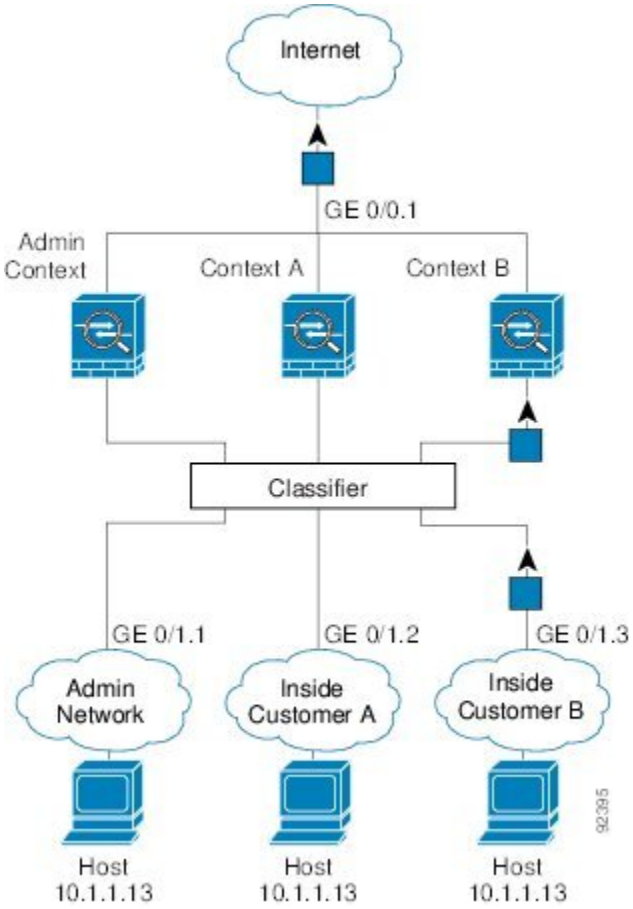
La figure suivante montre plusieurs contextes partageant une interface externe. Le classificateur affecte le paquet au contexte B, car le contexte B comprend l'adresse MAC à laquelle le routeur envoie le paquet.

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



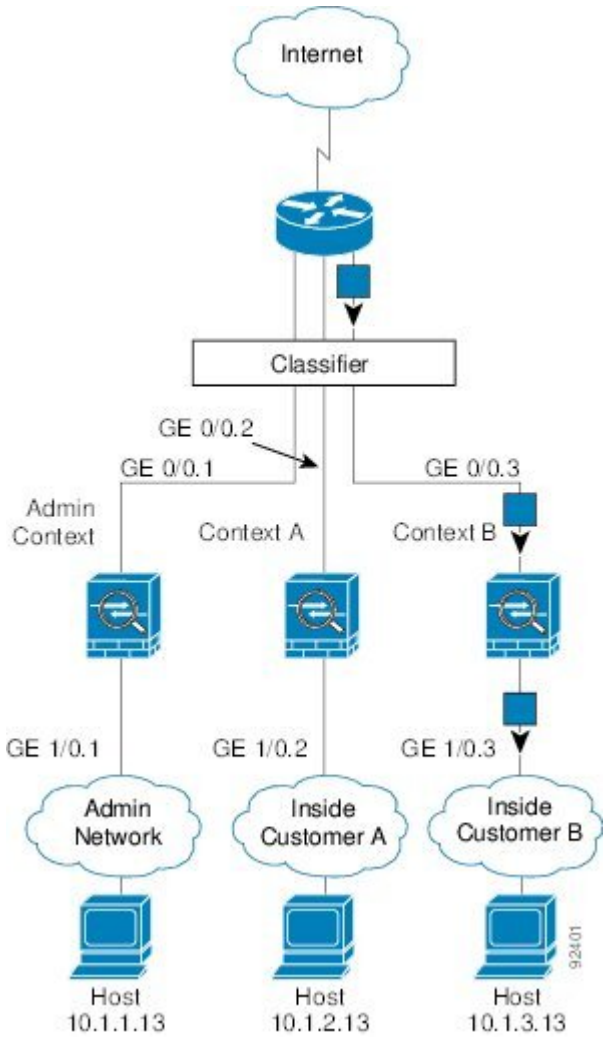

Notez que tout nouveau trafic entrant doit être classé, même en provenance des réseaux internes. La figure suivante montre un hôte sur le réseau interne du contexte B qui accède à Internet. Le classificateur affecte le paquet au contexte B, car l'interface d'entrée est Gigabit Ethernet 0/1.3, qui est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



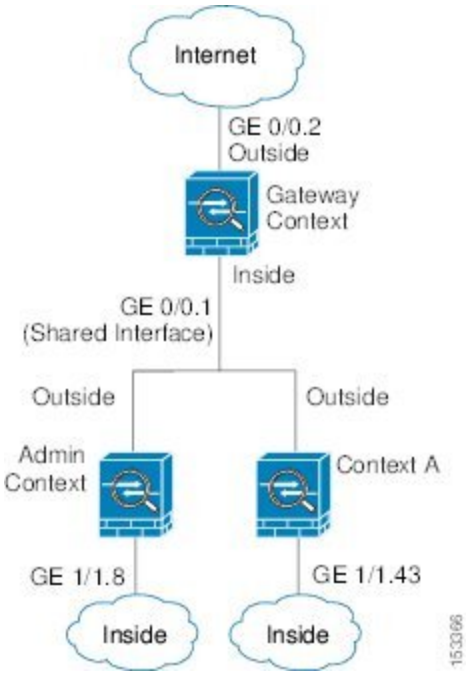

# Contextes de sécurité en cascade

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.

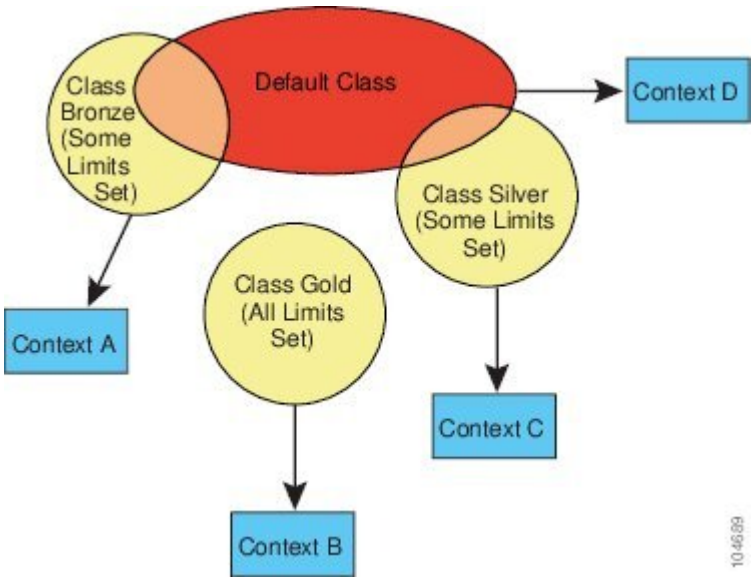
Si un contexte appartient à une autre classe que la classe par défaut, les paramètres de cette classe remplacent toujours les paramètres de la classe par défaut. Cependant, si l'autre classe a des paramètres non définis, le contexte membre utilise la classe par défaut pour ces limites. Par exemple, si 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.

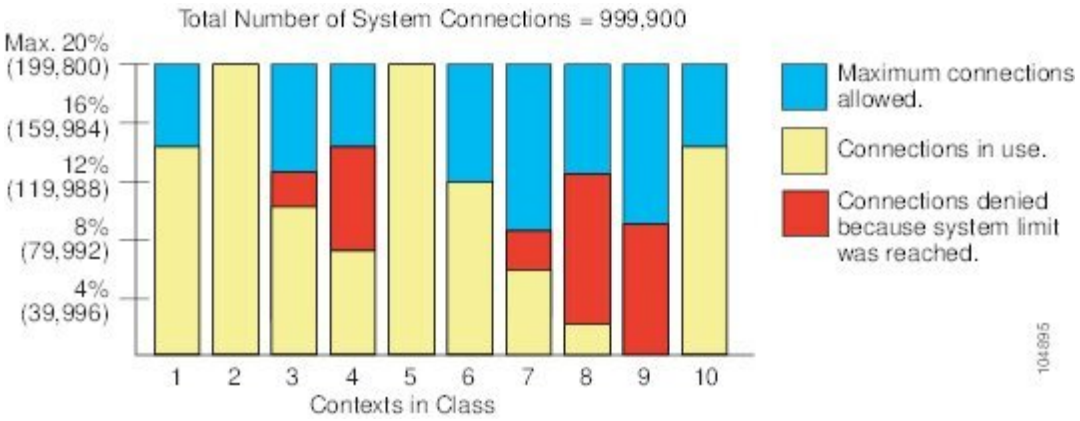
*Illustration 5 : Classes des ressources*




## 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*

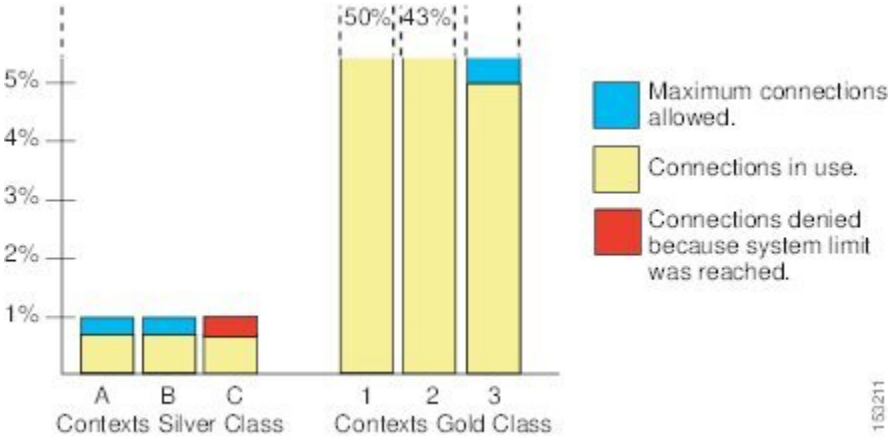



## Utiliser des ressources illimitées

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 33.

**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.<br>*Licence facultative, maximum :*<br>*Firepower 1120 : 5*<br>*Firepower 1140 : 10*<br>*Firepower 1150 : 25* |
| Firepower de la série 2100 | Licence Essentials : 2 contextes.<br>*Licence facultative, maximum :*<br>*Firepower 2110 : 25*<br>*Firepower 2120 : 25*<br>*Firepower 2130 : 30*<br>*Firepower 2140 : 40* |
| Secure Firewall 3100 | Licence Essentials : 2 contextes.<br>*Licence facultative, maximum :*<br>*Secure Firewall 3105 : 100*<br>*Secure Firewall 3110 : 100*<br>*Secure Firewall 3120 : 100*<br>*Secure Firewall 3130 : 100*<br>*Secure Firewall 3140 : 100* |
| Firepower 4100 | Licence Essentials : 10 contextes.<br>*Licence facultative : jusqu'à 250 contextes.* |
| Firepower 9300 | Licence Essentials : 10 contextes.<br>*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 auau 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 https://support.microsoft.com).
- 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 25

**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.

ASDM prend en charge le changement de mode, du mode unique au mode multiple, si vous utilisez l'assistant de haute disponibilité et d'évolutivité et que vous activez le basculement actif/actif. Consultez Basculement pour la haute disponibilité pour de plus amples renseignements. Si vous ne souhaitez pas utiliser le basculement actif/actif ou si vous souhaitez revenir en mode unique, vous devez changer de mode à l'aide de l'interface de ligne de commande; Comme le changement de mode nécessite une confirmation, vous ne pouvez pas utiliser l'outil de l'interface de ligne de commande. Cette section décrit les changements de mode au niveau de l'interface de ligne de commande.

## 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 Gérer les 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.



**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 |
|---|---|---|---|---|
| Sessions ASDM | Simultané | Au moins 1<br>5 au maximum | 200 | Sessions de gestion ASDM<br>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. |
| Connexions<br>Connexions/sec | Simultané ou taux | S. O. | Connexions simultanées : consultez Licences par modèle pour connaître la limite de connexions disponibles correspondant à votre modèle.<br>Taux : S.O. | Connexions TCP ou UDP entre deux hôtes, y compris les connexions entre un hôte et plusieurs autres hôtes.<br>**Remarque**<br>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/sec | Taux | s.o. | s.o. | nombre d'inspections d'applications par seconde |
| Entrées MAC | 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. |

| Nom de la ressource | Taux ou simultané | Nombre minimal et maximal par contexte | Limite du système | Description |
|---|---|---|---|---|
| Rafale Secure Client (services client sécurisés) | 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 Secure Client (services client sécurisés). | Le nombre de sessions Secure Client (services client sécurisés) autorisées au-delà de la quantité attribuée à un contexte avec Secure Client (services client sécurisés). Par exemple, si votre modèle prend en charge 5 000 homologues et que vous affectez 4 000 homologues dans tous les contextes avec Secure Client (services client sécurisés), les 1 000 sessions restantes sont disponibles pour Burst Secure Client (services client sécurisés). Contrairement à Secure Client (services client sécurisés), qui garantit les sessions au contexte, le Secure Client (services client sécurisés) Burst peut être surabonné; le groupement de rafales est disponible pour tous les contextes selon le principe du premier arrivé, premier servi. |
| Secure Client (services client sécurisés) | 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. |
| Autre rafale VPN | Simultané | S. O. | Le nombre de sessions Autre VPN correspondant à votre modèle moins la somme des sessions assignées à tous les contextes pour Autre VPN. | Le nombre de sessions VPN de site à site autorisées au-delà de la quantité attribuée à un contexte avec l'option Autre VPN. Par exemple, si votre modèle prend en charge 5 000 homologues et que vous affectez 4 000 homologues dans tous les contextes avec Autre VPN, les 1 000 sessions restantes sont disponibles pour Autre Rafale VPN. Contrairement à Autre VPN, qui garantit les sessions au contexte, Autre Rafale VPN peut être sursouscrit ; le groupement de rafales est disponible pour tous les contextes sur la base du premier arrivé, premier servi. |

| Nom de la ressource | Taux ou simultané | Nombre minimal et maximal par contexte | Limite du système | Description |
|---|---|---|---|---|
| Autre VPN | 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 SA en négociation | Simultané (pourcentage uniquement) | S. O. | Un pourcentage des autres sessions VPN attribuée à ce contexte. Consultez les ressources Autres VPN 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<br>5 au maximum | 100 | Séances SSH. |
| 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. |
| Syslogs/sec | Taux | s.o. | s.o. | Messages syslog par seconde. |
| Telnet | Simultané | Au moins 1<br>5 au maximum | 100 | Sessions Telnet. |
| Xlates | Simultané | S. O. | s.o. | Traduction d'adresses de réseau. |

### Procédure

**Étape 1** Si vous n'êtes pas déjà en mode de configuration système, dans le panneau **Device List (liste des périphériques)**, double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

**Étape 2** Choisissez **Configuration** > **Context Management** > **Resource Class**(classe de ressources de gestion du contexte de configuration) et cliquez sur **Add**(ajouter).

La boîte de dialogue **Add Resource Class** (ajouter une classe de ressource) apparaît.

**Étape 3** Saisissez un nom de classe de 20 caractères maximum dans le champ **Resource Class** (Classe de ressource).

**Étape 4** Dans la zone **Count Limited Resources** (Nombre de ressources limitées), définissez les limites simultanées de ressources.

Consultez le tableau précédent pour une description de chaque type de ressource.

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 ne définissez pas de limite, la limite est héritée de la classe par défaut. Si la classe par défaut ne définit pas de limite, la ressource est illimitée, ou égale à la limite du système, si elle est disponible. Pour la plupart des ressources, la valeur 0 fixe la limite à illimitée. Pour les types de VPN, 0 définit la limite à Aucun.

**Remarque** Si vous définissez également **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Gestion des accès)** > **Management Session Quota (Gestion des quotas de sessions)** dans un contexte pour définir le nombre maximal de sessions administratives (SSH, etc.), la valeur la plus basse sera utilisée.

**Étape 5** Dans la zone **Rate Limited Resource** (débit des ressources limitées), définissez la limite de débit des ressources.

Consultez le tableau précédent pour une description de chaque type de ressource.

Si vous ne définissez pas de limite, la limite est héritée de la classe par défaut. Si la classe par défaut ne définit pas de limite, elle est illimitée par défaut. 0 définit la limite à illimité.

**Étape 6** Cliquez sur **OK**.

# 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

### Procédure

**Étape 1** Si vous n'êtes pas déjà en mode de configuration système, dans le panneau **Device List (liste des périphériques)**, double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

**Étape 2** Choisissez **Configuration** > **Context Management (Gestion des contextes)** > **Security Contexts (Contexte de sécurité)**, puis cliquez sur **Add** (ajouter).

La boîte de dialogue**Add Context** (Ajouter un contexte) apparaît.

**Étape 3** Dans le champ **Security Context** (contexte de sécurité), saisissez le nom du contexte sous la forme d'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. « System » ou « Null » (en lettres majuscules ou minuscules) sont des noms réservés et ne peuvent pas être utilisés.

**Étape 4** Dans la zone **Interface Allocation** (attribution d'interface), cliquez sur le bouton **Add** (ajouter) pour affecter une interface au contexte.

a) Dans la liste déroulante **Interfaces (interfaces)** > **Physical interfaces (interfaces physiques)**, choisissez une interface.

Vous pouvez affecter l'interface principale, auquel cas vous laissez l'ID de sous-interface vide, ou vous pouvez affecter une sous-interface ou une plage de sous-interfaces associées à cette interface. En mode transparent de pare-feu, seules les interfaces qui n'ont pas été allouées à d'autres contextes sont affichées. Si l'interface principale était déjà affectée à un autre contexte, vous devez choisir une sous-interface.

b) (Facultatif) Dans la liste déroulante **Interfaces** > **Subinterface range** (plage de sous-interfaces) choisissez un ID de sous-interface.

Pour une plage d'ID de sous-interface, choisissez l'ID de fin dans la deuxième liste déroulante, si elle est disponible.

En mode transparent de pare-feu, seules les sous-interfaces qui n'ont pas été allouées à d'autres contextes sont affichées.

c) (Facultatif) Dans la zone des **noms d'alias**, cochez la case **Use Aliased Name in Context** (Utiliser un nom d'alias dans le contexte) pour définir un nom d'alias pour cette interface à utiliser dans la configuration de contexte au lieu de l'ID de l'interface.

- Dans le champ **Name** (nom), définissez le nom d'alias.

  Un nom d'alias doit commencer par une lettre, se terminer par une lettre et avoir comme caractères internes uniquement des lettres, des chiffres ou un trait de soulignement. Ce champ vous permet de spécifier un nom qui se termine par une lettre ou un trait de soulignement; pour ajouter un chiffre facultatif après le nom, définissez le chiffre dans le champ Plage.

- (Facultatif) Dans le champ **Range** (Plage), définissez le suffixe numérique du nom d'alias.

  Si vous avez une plage de sous-interfaces, vous pouvez entrer une plage de chiffres à ajouter au nom.

d) (Facultatif) Cochez la case **Show Hardware Properties in Context** (Afficher les propriétés matérielles dans le contexte) pour permettre aux utilisateurs du contexte de voir les propriétés de l'interface physique même si vous définissez un nom d'alias.

e) Cliquez sur **OK** pour revenir à la boîte de dialogue **Add Context** (ajouter un contexte).

**Étape 5** (Facultatif) Dans la zone **Resource Assignment** (Affectation des ressources), choisissez un nom de classe dans la liste déroulante **Resource Class** (Classe de ressources) pour affecter ce contexte à une classe de ressources.

Vous pouvez ajouter ou modifier une classe de ressources directement à partir de cette zone.

**Étape 6** Dans la liste déroulante **Config URL** (URL de configuration), choisissez un type de système de fichiers. Dans le champ, identifiez l'URL de l'emplacement de configuration du contexte.

Par exemple, l'URL combinée pour FTP a le format suivant :

ftp://server.example.com/configs/admin.cfg

**Étape 7** (Facultatif) Cliquez sur **Login** (Connexion) pour définir le nom d'utilisateur et le mot de passe pour les systèmes de fichiers externes.

**Étape 8** (Facultatif) Dans la liste déroulante **Failover Group** (Groupe de basculement), choisissez le nom du groupe pour définir le groupe de basculement pour le basculement actif/actif.

**Étape 9** (Facultatif) Pour **Cloud Web Security**, cliquez sur **Enable** (activer) pour activer l'inspection de Web Security dans ce contexte. Pour remplacer les licences définies dans la configuration système, saisissez une licence dans le champ **License** (Licence).

**Étape 10** (Facultatif) Ajoutez une description dans le champ **Description**.

**Étape 11** (Facultatif) Dans la zone **Storage URL AAssignment** (Affectation d'URL de stockage), vous pouvez 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) et les personnalisations de portails VPN SSL 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 et partagé 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 des **outils** > **de gestion de fichiers**.

a) Cochez la case **Configure private storage assignment** (Configurer l'affectation du stockage privé) et dans la liste déroulante **Sélect** (Sélectionner), choisissez le répertoire de stockage privé. Vous pouvez spécifier un espace de stockage privé 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). Sous le chemin spécifié, l'ASA crée un sous-répertoire du nom du contexte. Par exemple, pour contexteA, si vous spécifiez **disk1:/private-storage** comme chemin, l'ASA crée un sous-répertoire pour ce contexte à l'emplacement **disk1:/private-storage/contextA/**. Vous pouvez également nommer le chemin dans le contexte en saisissant un nom dans le champ **est mappé à** afin que le système de fichiers ne soit pas rendu visible aux administrateurs de contexte. Par exemple, si vous spécifiez le nom mappé **contexte**, dans le contexte, ce répertoire est appelé **contexte:**. Pour contrôler la quantité d'espace disque autorisée par contexte, consultez Configurer une classe pour la gestion des ressources, à la page 18.

b) Cochez la case **Configure Shared Storage Affectation** (Configurer l'affectation du stockage partagé) et dans la liste déroulante **Select** (Sélectionner), choisissez le répertoire de stockage partagé. 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 12** Cliquez sur **OK** pour revenir au volet **Security Contexts** (Contextes de sécurité).

**Étape 13** (Facultatif) Sélectionnez le contexte et cliquez sur **Change Firewall Mode** (modifier le mode de pare-feu) pour définir le mode de pare-feu transparent.

S'il s'agit d'un nouveau contexte, il n'y a aucune configuration à effacer. Cliquez sur**Change Mode** (Modifier le mode) pour passer en mode transparent de pare-feu.

S'il s'agit d'un contexte existant, veillez à sauvegarder la configuration avant de modifier le mode.

**Remarque** Vous ne pouvez pas modifier le mode du contexte actuellement connecté dans ASDM (généralement, le contexte d'administration); consultez Définir le mode du pare-feu (mode unique) pour définir le mode à l'aide de la ligne de commande.

**Étape 14** (Facultatif) Pour personnaliser la génération automatique des adresses MAC, consultez Attribuer automatiquement des adresses MAC aux interfaces de contexte, à la page 25.

**Étape 15** (Facultatif) Cochez la case **Specify the maximum number of TLS Proxy sessions that the ASA needs to support** (Précisez le nombre maximal de sessions mandataires TLS que l'ASA doit prendre en charge) pour spécifier le nombre maximal de sessions de serveur mandataire TLS pour le périphérique. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

# 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 nom de 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

**Étape 1** Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

**Étape 2** Choisissez **Configuration** > **Context Management** > **Security Contexts** et cochez **Mac-Address auto**. Si vous n'écrivez pas de préfixe, l'ASA génère automatiquement ce dernier en fonction des deux derniers octets.

**Étape 3** (Facultatif) Cochez la case **Prefix** (préfixe) et dans le champ, saisissez une valeur décimale 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 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.

### Procédure

**Étape 1** Dans le panneau Device List (Liste des périphériques), double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif pour configurer le système.

**Étape 2** Dans le volet Device List (Liste des périphériques), double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif pour configurer un contexte.

# 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.

**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.

### Avant de commencer

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

### Procédure

**Étape 1** Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

**Étape 2** Choisissez **Configuration** > **Context Management (Gestion des contextes)** > **Security Contexts (Contextes de sécurité)**.

**Étape 3** Sélectionnez le contexte que vous souhaitez supprimer, et cliquez sur **Delete** (Supprimer).

La boîte de dialogue Delete Context (Supprimer un contexte) apparaît.

**Étape 4** Si vous souhaitez peut-être rajouter ce contexte ultérieurement et conserver le fichier de configuration pour une utilisation future, décochez la case **Also delete config URL file from the disk** (Supprimer également le fichier d'URL de configuration du disque).

Si vous souhaitez supprimer le fichier de configuration, laissez la case cochée.

**Étape 5** Cliquez sur **Yes** (Oui).

# 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.



**Remarque** Pour ASDM, vous ne pouvez pas modifier le contexte d'administration dans ASDM, car votre session ASDM se déconnecterait. Vous pouvez effectuer cette procédure à l'aide de l'outil d'interface de ligne de commande, en notant que vous devrez vous reconnecter au nouveau contexte d'administration.

### 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

**Étape 1** Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

**Étape 2** Choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

La boîte de dialogue Command Line Interface (Interface de ligne de commande) apparaît.

**Étape 3** Entrez la commande suivante :

**admin-context** *context_name*

**Étape 4** Cliquez sur **Send** (envoyer).

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

**Remarque** 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** Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

**Étape 2** Choisissez **Configuration** > **Context Management (Gestion des contextes)** > **Security Contexts (Contextes de sécurité)**.

**Étape 3** Sélectionnez le contexte que vous souhaitez modifier, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit Context (Modifier le contexte) apparaît.

**Étape 4** Saisissez une nouvelle URL dans le champ Config URL (Configurer l'URL), puis cliquez sur **OK**.

Le système charge immédiatement le contexte pour qu'il s'exécute.

# 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** Dans le volet Device List (Liste des périphériques), double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

**Étape 2** Choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

La boîte de dialogue Command Line Interface (Interface de ligne de commande) apparaît.

**Étape 3** Entrez la commande suivante :

**clear configure all**

**Étape 4** Cliquez sur **Send** (envoyer).

La configuration du contexte est effacée.

**Étape 5** Choisissez à nouveau **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

La boîte de dialogue Command Line Interface (Interface de ligne de commande) apparaît.

**Étape 6** Entrez la commande suivante :

**copy startup-config running-config**

**Étape 7** Cliquez sur **Send** (envoyer).

L'ASA recharge la configuration. 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 26. Assurez-vous de décocher la case **Also delete config URL file from the disk** (Supprimer également le fichier d'URL de configuration du disque).

**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.

## Superviser l'utilisation des ressources de contexte

**Procédure**

**Étape 1** Si vous n'êtes pas déjà en mode système, dans le volet Device List (Liste des périphériques), double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

**Étape 2** Cliquez sur le bouton **Monitoring** (Supervision) dans la barre d'outils.

**Étape 3** Cliquez sur **Context Resource Usage** (Utilisation des ressources de contexte).

Cliquez sur chaque type de ressource pour afficher l'utilisation des ressources pour tous les contextes :

- **ASDM/Telnet/SSH** : affiche l'utilisation des connexions ASDM, Telnet et SSH.
  - Contexte : affiche le nom de chaque contexte.

    Pour chaque méthode d'accès, consultez les statistiques d'utilisation suivantes :
  - Connexions existantes (#) : affiche le nombre de connexions existantes.
  - External Connections (%) (Connexions existantes (%)) : affiche les connexions utilisées par ce contexte en tant que pourcentage du nombre total de connexions utilisées par tous les contextes.
  - Pic de connexions (#) : affiche le pic de connexions depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.
- **Routes** : affiche l'utilisation des routes dynamiques.
  - Contexte : affiche le nom de chaque contexte.
  - Connexions existantes (#) : affiche le nombre de connexions existantes.
  - External Connections (%) (Connexions existantes (%)) : affiche les connexions utilisées par ce contexte en tant que pourcentage du nombre total de connexions utilisées par tous les contextes.
  - Pic de connexions (#) : affiche le pic de connexions depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.

- **Xlates** : affiche l'utilisation des traductions d'adresses réseau.
  - Contexte : affiche le nom de chaque contexte.
  - Xlates (#) : affiche le nombre de xlates actuels.
  - Xlates (%) : affiche les xlates utilisés par ce contexte en tant que pourcentage du nombre total de xlates utilisés par tous les contextes.
  - Pic (#) : affiche le pic de xlates depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.
- **NAT** : affiche le nombre de règles NAT.
  - Contexte : affiche le nom de chaque contexte.
  - NATs (#) : affiche le nombre actuel de règles NAT.
  - NATs (%) : affiche les règles NAT utilisées par ce contexte en tant que pourcentage du nombre total de règles NAT utilisées par tous les contextes.
  - Pic de NAT (#) : affiche le pic de NAT depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.
- **Journaux système** : affiche le taux de messages du journal système.
  - Contexte : affiche le nom de chaque contexte.
  - Taux de journal système (#/sec) : affiche le taux actuel de messages du journal du système.
  - Taux de journal système (%) : affiche les messages du journal système générés par ce contexte en pourcentage du nombre total de messages de journal système générés par tous les contextes.
  - (Taux maximum de journal système) : affiche le taux maximum de messages du journal système depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage** , soit en raison du redémarrage du périphérique.
- VPN : affiche l'utilisation des tunnels VPN de site à site.
  - Contexte : affiche le nom de chaque contexte.
  - Connexions VPN : affiche l'utilisation des sessions VPN garanties.
  - Connexions de VPN en rafale : affiche l'utilisation des sessions VPN en rafale.
    - Existant (#) : affiche le nombre de tunnels existants.
    - Pic (#) : affiche le pic de tunnels depuis la dernière suppression des statistiques, soit à l'aide de la commande **clear resource usage**, soit à la suite du redémarrage du périphérique.

**Étape 4** Cliquez sur **Refresh** (Actualiser) pour actualiser la vue.

# 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

**Étape 1** Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

**Étape 2** Choisissez **Configuration** > **Contexte Management (Gestion de contextes)** > **Security Contextes (Contextes de sécurité)** et affichez les colonnes Primary MAC (MAC principale) et Secondary MAC (MAC secondaire).

## Afficher les adresses MAC dans un contexte

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

### Procédure

**Étape 1** Si vous n'êtes pas déjà en mode de configuration système, dans le panneau Device List (liste des périphériques), double-cliquez sur **System** (système) sous l'adresse IP du périphérique actif.

**Étape 2** Choisissez **Configuration** > **Interfaces** et affichez la colonne d'adresses MAC.

Ce tableau 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.

# Historique du mode de contexte multiple

***Tableau 2 : 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.<br>Nous avons introduit les écrans suivants : Configuration > Context Management (Gestion des contextes). |
| Affectation automatique de l'adresse MAC | 7.2(1) | L'affectation automatique de l'adresse MAC aux interfaces de contexte a été introduite.<br>Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité). |
| Gestion des ressources | 7.2(1) | La gestion des ressources a été introduite.<br>Nous avons introduit l'écran suivant : Configuration > Context Management (Gestion des contextes) > Resource Management (Gestion des ressources). |
| 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.<br>Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité). |
| Améliorations de l'affectation automatique de l'adresse MAC | 8.0(5)/8.2(2) | Le format de l'adresse MAC a été modifié pour utiliser un préfixe, une valeur initiale fixe (A2) et un schéma différent pour les adresses MAC des unités principale et secondaire dans une paire de basculement. Les adresses MAC sont également conservées de façon permanente pendant les rechargements. L'analyseur de commande vérifie maintenant si la génération automatique est activée; si vous souhaitez également attribuer manuellement une adresse MAC, vous ne pouvez pas commencer l'adresse MAC manuelle par A2.<br>Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité). |
| Augmentation du nombre maximum de contextes pour les modèles ASA 5550 et 5580 | v 8.4(1) | Le nombre maximum de contextes de sécurité pour l'ASA 5550 est passé de 50 à 100. Le nombre maximum pour l'ASA 5580 est passé de 50 à 250. |
| Affectation automatique de l'adresse MAC activée par défaut | 8.5(1) | L'affectation automatique de l'adresse MAC est maintenant activée par défaut.<br>Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité). |

| 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. 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.<br>**Remarque**<br>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.<br>Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité) |
| 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.<br>Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité). |
| 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.<br>Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Resource Class (Classe de ressources) > Add Resource Class (Ajouter une classe de ressources) |
| 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. |

| Nom de la caractéristique | Versions de plateforme | Renseignements sur les fonctionnalités |
|---|---|---|
| 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.<br><br>Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Resource Class (Classe de ressources) > Add Resource Class (Ajouter une classe de ressources) |
| 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.<br><br>Nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Resource Class (Classe de ressources) > Add Resource Class (Ajouter une classe de ressources) |
| 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 :<br>• AnyConnect 3.x ou versions ultérieures (SSL VPN uniquement; pas de prise en charge d'IKEv2)<br>• Configuration centralisée de l'image Secure Client (services client sécurisés)<br>• Mise à niveau de l'image Secure Client (services client sécurisés)<br>• Gestion des ressources de contexte pour les connexions Secure Client (services client sécurisés)<br><br>**Remarque**<br>La licence Secure Client Premier est requise pour le mode de contexte multiple; vous ne pouvez pas utiliser la licence par défaut ou existante.<br><br>Nous avons modifié l'écran suivant : **Configuration** > **Context Management (Gestion des contextes)** > **Resource Class (Classe de ressources)** > **Add Resource Class (Ajouter une classe de ressources)** |
| 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.<br><br>Nous n'avons pas modifié d'écrans. |

| Nom de la caractéristique | Versions de plateforme | Renseignements sur les fonctionnalités |
|---|---|---|
| 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 :<br>• Stockage privé : stockez les fichiers associés uniquement à cet utilisateur et spécifiques au contenu que vous souhaitez pour cet utilisateur.<br>• 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.<br>Nous avons modifié les écrans suivants : **Configuration** > **Context Management (Gestion des contextes)** > **Resource Class (Classe de ressources)** > **Add Resource Class (Ajouter une classe de ressources)**<br>**Configuration** > **Context Management (Gestion des contextes)** > **Security Contexts (Contextes de sécurité)** |
| 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.<br>Nous n'avons pas modifié d'écrans. |
| 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.<br>Nous n'avons pas modifié d'écrans. |
| 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.<br>Nous n'avons pas modifié d'écrans. |
| 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.<br>Nous n'avons pas modifié d'écrans. |
| 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. |

| Nom de la caractéristique | Versions de plateforme | Renseignements sur les fonctionnalités |
|---|---|---|
| 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.<br><br>Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Management Session Quota (Quota de sessions de gestion)** |
| 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.