

Logiciels et configurations

Ce chapitre décrit comment gérer le logiciel et les configurations ASA.

- Mettre à niveau le logiciel, à la page 1
- Charger une image à l'aide de ROMMON (ISA 3000), à la page 1
- Mettre à niveau l'image ROMMON : ISA 3000, à la page 3
- Rétrograder votre logiciel, à la page 4
- Gérer les fichiers, à la page 9
- Définir l'image ASA, ASDM et la configuration de démarrage, à la page 17
- Sauvegarde et restauration de configurations ou d'autres fichiers, à la page 19
- Programmer un redémarrage du système, à la page 26
- Échange à chaud d'un SSD sur Cisco Secure Firewall , à la page 27
- Historique des logiciels et des configurations, à la page 29

Mettre à niveau le logiciel

Consultez le Guide de mise à niveau de Cisco ASA pour accéder aux procédures de mise à niveau complètes.

Charger une image à l'aide de ROMMON (ISA 3000)

Pour charger une image logicielle sur un ASA en mode ROMMON à l'aide de TFTP, procédez comme suit.

Procédure

Étape 1 Connectez-vous au port de la console de l'ASA en suivant les instructions de Accéder à la console de l'ISA 3000.

Étape 2 Mettez l'ASA hors tension, puis rallumez-le.

Étape 3 Pendant le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à passer en mode ROMMON.

Étape 4 En mode ROMMON, définissez les paramètres d'interface avec l'ASA, notamment l'adresse IP, l'adresse du serveur TFTP, l'adresse de la passerelle, le fichier d'image logicielle et le port, comme suit :

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
```

```
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

Remarque Assurez-vous que la connexion au réseau est déjà établie.

Sur les plateformes ASA 5506-X, ASA 5508-X, ASA 5516-X et ISA 3000, la commande **interface** ne fonctionne pas, ce qui oblige à utiliser l'interface Management 1/1 pour la récupération TFTP.

Étape 5 Validez les paramètres :

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

Étape 6 Envoyez un message Ping au serveur TFTP :

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

Étape 7 Enregistrez les paramètres réseau pour une utilisation ultérieure :

```
rommon #8> sync
Updating NVRAM Parameters...
```

Étape 8 Chargez l'image logicielle :

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes
```

```
Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

Une fois l'image logicielle chargée, l'ASA quitte automatiquement le mode ROMMON.

Étape 9 Le démarrage de l'ASA en mode ROMMON ne permet pas de conserver l'image du système après un rechargement. Vous devez donc télécharger l'image dans la mémoire flash. Consultez le Guide de mise à niveau de Cisco ASA pour accéder aux procédures de mise à niveau complètes.

Mettre à niveau l'image ROMMON : ISA 3000

Pour les ISA 3000, procédez comme suit afin de mettre à niveau l'image ROMMON. Pour les modèles ASA, vous devez avoir installé la version 1.1.8 ou toute version ultérieure de ROMMON sur votre système. Nous vous recommandons d'effectuer la mise à niveau vers la dernière version.

Seule une mise à niveau vers une nouvelle version est possible; la rétrogradation n'est pas prise en charge.

Mise en garde La ISA 3000 prend deux fois plus de temps que pour les versions précédentes (environ 15 minutes). **N'éteignez pas** l'appareil pendant la mise à niveau. Si la mise à niveau prend plus de 30 minutes ou si elle échoue, contactez l'assistance technique de Cisco. **N'éteignez pas** l'appareil et ne le réinitialisez pas.

Avant de commencer

Procurez-vous la nouvelle image ROMMON sur Cisco.com et enregistrez-la sur un serveur pour ensuite la copier sur l'ASA. L'ASA prend en charge les serveurs FTP, TFTP, SCP, HTTP(S) et SMB. Téléchargez l'image de :

- ISA 3000 : https://software.cisco.com/download/home/286288493/type

Procédure

Étape 1 Copiez l'image ROMMON sur la mémoire flash de l'ASA. Cette procédure illustre la commande « copy FTP ». Entrez **copy ?** pour la syntaxe appropriée pour les autres types de serveurs.

copy ftp://[*noms d'utilisateur***:***mot de passe***@**]*server_ip*/**asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

Étape 2 Pour connaître la version installée, entrez la commande **show module** et consultez la version du pare-feu (FW) dans la sortie du module 1 du tableau des plages d'adresses MAC :

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
```

```
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

Étape 3 Procédez à la mise à niveau de l'image ROMMON :

upgrade rommon disk0:asa5500-firmware-*XXXX*.SPA

Exemple :

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

Étape 4 Lorsque vous y êtes invité, appuyez sur Confirmer pour recharger l'ASA.

L'ASA met à niveau l'image ROMMON, puis recharge le système d'exploitation.

Rétrograder votre logiciel

Dans de nombreux cas, vous pouvez rétrograder votre logiciel ASA et restaurer une configuration de sauvegarde à partir de la version de logiciel précédemment installée. La méthode de rétrogradation dépend de votre plateforme ASA.

Directives et limites en matière de rétrogradation

Consultez les consignes suivantes avant la rétrogradation :

- **Il n'y a pas de prise en charge officielle de la rétrogradation sans temps d'arrêt pour la mise en grappe**. Cependant la rétrogradation sans temps d'arrêt fonctionnera dans certains cas. Si vous rencontrez des problèmes, vous devez recharger vos unités de grappe, ce qui entraîne un temps d'arrêt.

- **Problème de rétrogradation de la version 9.18 ou ultérieure** : il y a un changement de comportement dans la version 9.18 où la commande **access-group** sera répertoriée avant ses commandes **access-list**. Si vous effectuez une rétrogradation, la commande **access-group** sera rejetée, car elle n'a pas encore chargé les commandes **access-list**. Ce résultat se produit même si vous avez précédemment activé la commande **forward-reference enable**, car cette commande est maintenant supprimée. Avant de procéder à la rétrogradation, assurez-vous de copier toutes les commandes **access-group** manuellement, puis après la rétrogradation, saisissez-les de nouveau.
- **Les tunnels VPN sont répliqués sur l'unité de secours même si cette dernière exécute une version du logiciel qui ne prend pas en charge la suite de chiffrement que le tunnel d'origine a négociée.** Ce scénario se produit lors de la rétrogradation. Dans ce cas, déconnectez votre connexion VPN et reconnectez-vous.

Configuration incompatible supprimée après la rétrogradation

Lorsque vous effectuez une rétrogradation à une ancienne version, les commandes qui ont été introduites dans les versions ultérieures seront supprimées de la configuration. Il n'existe aucun moyen automatisé de vérifier la configuration par rapport à la version cible avant de procéder à la rétrogradation. Vous pouvez découvrir quand de nouvelles commandes ont été ajoutées dans les nouvelles fonctionnalités d'ASA par version.

Vous pouvez afficher les commandes rejetées *après* avoir effectué une rétrogradation en utilisant la commande **show startup-config errors**. Si vous pouvez rétrograder un périphérique de laboratoire, vous pouvez prévisualiser les effets en utilisant cette commande avant de rétrograder un périphérique de production.

Dans certains cas, l'ASA migre automatiquement les commandes vers de nouveaux formulaires lors de la mise à niveau. Ainsi, selon votre version, même si vous n'avez pas configuré manuellement de nouvelles commandes, la rétrogradation peut être influencée par les migrations de configuration. Nous vous recommandons de sauvegarder votre ancienne configuration logicielle afin de pouvoir l'utiliser lors de la rétrogradation. Dans le cas d'une mise à niveau vers la version 8.3, une sauvegarde est automatiquement créée (<old_version>_startup_cfg.sav). Les autres migrations ne créent pas de sauvegardes. Consultez les « Directives et migrations propres à la version » dans le guide de mise à niveau d'ASA pour en savoir plus sur les migrations automatiques des commandes qui pourraient avoir une incidence sur la rétrogradation.

Consultez également les problèmes de rétrogradation connus dans Directives et limites en matière de rétrogradation, à la page 4.

Par exemple, un ASA utilisant la version 9.8(2) inclut les commandes suivantes :

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

Lorsque vous rétrogradez le périphérique à la version 9.0(4), les erreurs suivantes s'afficheront au démarrage :

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
                                  ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                                ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

```
                                                ^
ERROR: % Invalid input detected at '^' marker.
```

Dans cet exemple, la prise en charge de **sctp** dans la commande **access-list étendue** a été ajoutée dans la version 9.5(2), la prise en charge de **pbkdf2** dans la commande **username** a été ajoutée dans la version 9.6(1) et la prise en charge de **engineID** dans la commande **snmp-server user** a été ajouté dans la version 9.5(3).

Rétrograder l'appareil ASA

Vous pouvez rétrograder la version du logiciel de l'ASA en définissant la version de l'ASA sur l'ancienne version, en restaurant la configuration de sauvegarde dans la configuration de démarrage, puis en la rechargeant. Cette procédure s'applique aux modèles suivants :

- Firepower 1000
- Secure Firewall 1200
- Firepower de la série 2100
- Secure Firewall 3100
- Secure Firewall 4200

Avant de commencer

Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration. Si vous ne restaurez pas l'ancienne configuration, vous risquez d'avoir des commandes incompatibles représentant des fonctionnalités nouvelles ou modifiées. Toute nouvelle commande sera rejetée lorsque vous chargerez l'ancienne version du logiciel.

Procédure

Étape 1 Chargez l'ancienne version du logiciel ASA en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe. Dans ce cas, précisez l'ancienne version d'ASA au lieu d'une nouvelle version. **Important :** Ne rechargez *pas* encore l'ASA.

Étape 2 Au niveau de l'interface de ligne de commande de l'ASA, copiez la configuration de l'ASA de secours dans la configuration de démarrage. Pour le basculement, effectuez cette étape sur l'unité active. Cette étape réplique la commande sur l'unité de secours.

copy *ancienne_url_de_configuration* **startup-config**

Il est important que vous n'enregistriez pas la configuration en cours dans la configuration de démarrage à l'aide de **write memory**; cette commande remplacera votre configuration de sauvegarde.

Exemple :

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

Étape 3 Rechargez l'ASA.

Interface de ligne de commande ASA

reload

ASDM

Choisissez **Tools (Outils)** > **System Reload (Rechargement du système)**.

Rétrograder le Firepower 2100 en mode plateforme

Vous pouvez rétrograder la version du logiciel de l'ASA en restaurant la configuration de sauvegarde à la configuration de lancement, en réglant la version de l'ASA à l'ancienne version, puis en rechargeant l'unité.

Avant de commencer

Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration. Si vous ne restaurez pas l'ancienne configuration, vous risquez d'avoir des commandes incompatibles représentant des fonctionnalités nouvelles ou modifiées. Toute nouvelle commande sera rejetée lorsque vous chargerez l'ancienne version du logiciel.

Procédure

Étape 1 Au niveau de l'interface de ligne de commande de l'ASA, copiez la configuration de l'ASA de secours dans la configuration de démarrage. Pour le basculement, effectuez cette étape sur l'unité active. Cette étape réplique la commande sur l'unité de secours.

copy *ancienne_url_de_configuration* **startup-config**

Il est important que vous n'enregistriez pas la configuration en cours dans la configuration de démarrage à l'aide de **write memory**; cette commande remplacera votre configuration de sauvegarde.

Exemple :

```
ciscoasa# copy disk0:/9.12.4_cfg.sav startup-config
```

Étape 2 Dans FXOS, utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour utiliser l'ancienne version du logiciel ASA en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe. Dans ce cas, précisez l'ancienne version d'ASA au lieu d'une nouvelle version.

Rétrograder le Firepower 4100/9300

Vous pouvez rétrograder la version du logiciel de l'ASA en restaurant la configuration de sauvegarde à la configuration de lancement, en réglant la version de l'ASA à l'ancienne version, puis en rechargeant l'unité.

Avant de commencer

- Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration. Si vous ne restaurez pas l'ancienne configuration, vous risquez d'avoir des commandes incompatibles représentant des fonctionnalités nouvelles ou modifiées. Toute nouvelle commande sera rejetée lorsque vous chargerez l'ancienne version du logiciel.

- Assurez-vous que l'ancienne version de l'ASA est compatible avec la version de FXOS actuelle. Si ce n'est pas le cas, rétrogradez FXOS en premier lieu avant de restaurer l'ancienne configuration ASA. Assurez-vous que l'instance rétrogradée de FXOS est également compatible avec la version d'ASA actuelle (avant de la rétrograder). Si vous ne parvenez pas à assurer la compatibilité, nous vous conseillons de ne pas procéder à une rétrogradation.

Procédure

Étape 1 Au niveau de l'interface de ligne de commande de l'ASA, copiez la configuration de l'ASA de secours dans la configuration de démarrage. Pour le basculement ou la mise en grappe, effectuez cette étape sur l'unité active/de contrôle. Cette étape réplique la commande sur les unités de secours/de données.

copy *ancienne_url_de_configuration* **startup-config**

Il est important que vous n'enregistriez pas la configuration en cours dans la configuration de démarrage à l'aide de **write memory**; cette commande remplacera votre configuration de sauvegarde.

Exemple :

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

Étape 2 Dans FXOS, utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour utiliser l'ancienne version du logiciel ASA en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe. Dans ce cas, précisez l'ancienne version d'ASA au lieu d'une nouvelle version.

Étape 3 Si vous rétrogradez également FXOS, utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour définir l'ancienne version du logiciel FXOS pour qu'elle soit la version actuelle en suivant la procédure de mise à niveau du guide de mise à niveau ASA pour les déploiements autonomes, de basculement ou de mise en grappe.

Rétrograder l'ISA 3000

La fonctionnalité de rétrogradation fournit un raccourci pour effectuer les fonctions suivantes sur les modèles ISA 3000 :

- Effacement de la configuration de l'image de démarrage (**clear configure boot**).
- Définition de l'image de démarrage comme étant l'ancienne image (**boot system**).
- (Facultatif) Entrée d'une nouvelle clé d'activation (**activation-key**).
- Enregistrement de la configuration en cours pour le démarrage (**write memory**). Cette opération définit la variable d'environnement BOOT sur l'ancienne image, de sorte que lorsque vous rechargez, l'ancienne image est chargée.
- Copie de l'ancienne sauvegarde de configuration dans la configuration de démarrage (**copy** *ancienne_url_de_configuration* **startup-config**).
- Rechargement (**reload**).

Avant de commencer

- Cette procédure requiert une configuration de sauvegarde de l'ASA avant la mise à niveau, afin que vous puissiez restaurer l'ancienne configuration.

Procédure

Étape 1 choisissez **Outils** > **Rétrograder le logiciel**.

La boîte de dialogue Rétrograder le logiciel s'affiche.

Étape 2 Pour l'**image ASA**, cliquez sur **Sélectionner un fichier d'image**.

La boîte de dialogue **Parcourir les emplacements des fichiers** s'affiche.

Étape 3 Cliquez sur l'un des boutons radio suivants :

- **Serveur distant** : choisissez ftp, smb ou http dans la liste déroulante, puis saisissez le chemin d'accès à l'ancien fichier image.
- **Système de fichiers flash** : cliquez sur **Parcourir la mémoire flash** pour choisir l'ancien fichier image sur le système de fichiers flash local.

Étape 4 Pour la **configuration**, cliquez sur **Parcourir la mémoire flash** pour choisir le fichier de configuration de pré-migration.

Étape 5 (Facultatif) Dans le champ **Clé d'activation**, saisissez l'ancienne clé d'activation si vous devez rétablir une clé d'activation antérieure à la version 8.3.

Étape 6 Cliquez sur **Rétrograder**.

Gérer les fichiers

ASDM fournit un ensemble d'outils de gestion de fichiers pour vous aider à effectuer des tâches de gestion de fichiers de base. L'outil de gestion de fichiers vous permet d'afficher, de déplacer, de copier et de supprimer des fichiers stockés dans la mémoire flash, de transférer des fichiers et de gérer des fichiers sur des périphériques de stockage distants (points de montage).

Remarque En mode de contexte multiple, cet outil est uniquement disponible dans le contexte de sécurité du système.

Configurer l'accès au fichier

L'ASA peut utiliser un client FTP, un client de copie sécurisée ou un client TFTP. Vous pouvez également configurer l'ASA en tant que serveur de copie sécurisée afin de pouvoir utiliser un client de copie sécurisée sur votre ordinateur.

Configurer le mode client FTP

L'ASA peut utiliser FTP pour charger ou télécharger des fichiers image ou des fichiers de configuration vers ou depuis un serveur FTP. En mode FTP passif, le client initie à la fois la connexion de contrôle et la connexion de données. Le serveur, qui est le destinataire de la connexion de données en mode passif, répond par le numéro de port sur lequel il écoute pour la connexion spécifique.

Procédure

Étape 1 Dans le volet Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > FTP Client (Client FTP), cochez la case **Specify FTP mode as passive** (Spécifier le mode FTP comme passif).

Étape 2 Cliquez sur **Apply** (Appliquer).

La configuration du client FTP est modifiée et la modification est enregistrée dans la configuration en cours d'exécution.

Configurer l'ASA Secure Copy Client

Vous pouvez configurer les paramètres SCP à l'aide de la commande **copy**.

La performance de SCP dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier le chiffrement proposé, utilisez la commande **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)** ; par exemple, choisissez **Custom** (Personnalisé) et définissez-le sur aes128-cbc.

Avant de commencer

- La licence ASA doit avoir la licence de cryptage renforcé (3DES/AES) pour prendre en charge les connexions SSH version 2.
- Sauf indication contraire, pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, dans le volet Configuration > Device List (Liste des périphériques), double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.
- Pour le serveur SCP, activez SSH sur l'ASA conformément à Configurer l'accès SSH.

Procédure

Étape 1 Selon votre mode de contexte :

- Pour le mode unique, choisissez **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > Secure Copy (SCP) (Copie sécurisée (SCP))**.

- Pour le mode multiple dans le système, choisissez **Configuration > Device Management (Gestion des périphériques) > Device Administration (Administration des périphériques) > Secure Copy (Copie sécurisée)**

Étape 2 (Facultatif) L'ASA stocke la clé d'hôte SSH pour chaque serveur SCP auquel elle se connecte. Vous pouvez ajouter ou supprimer manuellement des serveurs et leurs clés de la base de données ASA si vous le souhaitez.

Pour ajouter une clé :

a) Cliquez sur **Add** (Ajouter) pour un nouveau serveur ou sélectionnez le serveur dans le tableau des hôtes SSH de confiance, puis cliquez sur **Edit** (Modifier).
b) Pour un nouveau serveur, dans le champ Host (Hôte), saisissez l'adresse IP du serveur.
c) Cochez la case **Add public key for the trusted SSH host** (Ajouter une clé publique pour l'hôte SSH de confiance).
d) Spécifiez l'une des clés suivantes :

- Fingerprint (empreinte) : saisissez la clé déjà hachée; par exemple, une clé que vous avez copiée à partir de la sortie de la commande **show**.
- Key (Clé) : saisissez la clé publique ou la valeur de hachage de l'hôte SSH. La chaîne de clés est la clé publique RSA codée en Base64 de l'homologue distant. Vous pouvez obtenir la valeur de clé publique à partir d'un client SSH ouvert; c'est-à-dire du fichier .ssh/id_rsa.pub. Après avoir soumis la clé publique codée en Base64, cette clé est ensuite hachée au moyen de SHA-256.

Pour supprimer une clé, sélectionnez le serveur dans le tableau des hôtes SSH de confiance, puis cliquez sur **Delete** (Supprimer).

Étape 3 (Facultatif) Pour être informé lorsqu'une nouvelle clé d'hôte est détectée, cochez la case **Inform me when a new host key is detected** (M'informer lorsqu'une nouvelle clé d'hôte est détectée).

Par défaut, cette option est activée. Lorsque cette option est activée, vous êtes invité à accepter ou à refuser la clé d'hôte si elle n'est pas déjà stockée sur l'ASA. Lorsque cette option est désactivée, l'ASA accepte automatiquement la clé d'hôte si elle n'a pas été stockée auparavant.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer le chemin du client TFTP pour l'ASA

Le TFTP est un protocole de transfert de fichiers client/serveur simple, qui est décrit dans les RFC 783 et RFC 1350, version 2. Vous pouvez configurer l'ASA en tant que client TFTP afin qu'il puisse copier des fichiers vers ou à partir d'un serveur TFTP. De cette façon, vous pouvez sauvegarder et propager des fichiers de configuration sur plusieurs ASA.

Cette section vous permet de prédéfinir le chemin d'accès à un serveur TFTP afin de ne pas avoir à le saisir dans des commandes telles que **copy** et **configure net**.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **File Access (Accès au fichier)** > **TFTP Client (Client TFTP)** et cochez la case **Enable** (Activer).

Étape 2 Dans la liste déroulante Interface Name (Nom de l'interface), choisissez l'interface à utiliser comme client TFTP.

Étape 3 Dans le champ IP Adress (Adresse IP), saisissez l'adresse IP du serveur TFTP sur lequel les fichiers de configuration seront enregistrés.

Étape 4 Dans le champ Path (Chemin), saisissez le chemin d'accès au serveur TFTP sur lequel les fichiers de configuration seront enregistrés.

Par exemple : /tftpboot/asa/config3

Étape 5 Cliquez sur **Apply**.

Ajouter des points de montage

Vous pouvez ajouter un point de montage CIFS ou FTP.

Ajouter un point de montage CIFS

Pour définir un point de montage Common Internet File System (CIFS), procédez comme suit.

Procédure

Étape 1 Sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **File Access (Accès au fichier)** > **Mount-Points (Points de montage)**, et cliquez sur **Add (Ajouter)** > **CIFS Mount Point (Point de montage CIFS)**.

La boîte de dialogue Add CIFS Mount Point (Ajouter un point de montage CIFS) apparaît.

Étape 2 Cochez la case **Enable mount point** (Activer le point de montage).

Cette option associe le système de fichiers CIFS de l'ASA à l'arborescence de fichiers UNIX.

Étape 3 Dans le champ Mount Point Name (Nom du point de montage), saisissez le nom d'un emplacement CIFS existant.

Étape 4 Dans le champ Server Name or IP Address (Nom de serveur ou adresse IP), saisissez le nom ou l'adresse IP du serveur sur lequel se trouve le point de montage.

Étape 5 Dans le champ Share Name (Nom de partage), saisissez le nom du dossier sur le serveur CIFS.

Étape 6 Dans le champ NT Domain Name (Nom de domaine NT), saisissez le nom du domaine NT dans lequel se trouve le serveur.

Étape 7 Dans le champ User Name (Nom d'utilisateur), saisissez le nom de l'utilisateur autorisé pour le montage du système de fichiers sur le serveur.

Étape 8 Dans le champ Password (Mot de passe), saisissez le mot de passe de l'utilisateur autorisé pour le montage du système de fichiers sur le serveur.

Étape 9 Dans le champ Confirm Password (Confirmer le mot de passe), ressaisissez le mot de passe.

Étape 10 Cliquez sur **OK**.

La boîte de dialogue Add CIFS Mount Point (Ajouter un point de montage CIFS) se ferme.

Étape 11 Cliquez sur **Apply** (Appliquer).

Ajouter un point de montage FTP

Pour un point de montage FTP, le serveur FTP doit avoir un style de listage des répertoires UNIX. Les serveurs FTP de Microsoft ont une valeur par défaut du style de listage des répertoires MS-DoS.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **File Access (Accès au fichier)** > **Mount-Points (Points de montage)**, et cliquez sur **Add (Ajouter)** > **FTP Mount Point (Point de montage FTP)**.

La boîte de dialogue Add FTP Mount Point (Ajouter un point de montage FTP) apparaît.

Étape 2 Cochez la case **Enable** (activer).

Cette option associe le système de fichiers FTP de l'ASA à l'arborescence de fichiers UNIX.

Étape 3 Dans le champ Mount Point Name (Nom du point de montage), saisissez le nom d'un emplacement FTP existant.

Étape 4 Dans le champ Server Name or IP Address (Nom de serveur ou adresse IP), saisissez le nom ou l'adresse IP du serveur où se trouve le point de montage.

Étape 5 Dans le champ Mode, cliquez sur le bouton radio du mode FTP (**Actif** ou **Passif**). Lorsque vous choisissez le mode passif, le client initie à la fois la connexion de contrôle FTP et la connexion de données. Le serveur répond par le numéro de son port d'écoute pour cette connexion.

Étape 6 Dans le champ Path to Mount (Chemin d'accès au montage), saisissez le nom du chemin d'accès au répertoire du serveur de fichiers FTP.

Étape 7 Dans le champ User Name (Nom d'utilisateur), saisissez le nom de l'utilisateur autorisé pour le montage du système de fichiers sur le serveur.

Étape 8 Dans le champ Password (Mot de passe), saisissez le mot de passe de l'utilisateur autorisé pour le montage du système de fichiers sur le serveur.

Étape 9 Dans le champ Confirm Password (Confirmer le mot de passe), ressaisissez le mot de passe.

Étape 10 Cliquez sur **OK**.

La boîte de dialogue Add FTP Mount Point (Ajouter un point de montage FTP) se ferme.

Étape 11 Cliquez sur **Apply** (Appliquer).

Accéder à l'outil de gestion de fichiers

Pour utiliser les outils de gestion de fichiers, procédez comme suit.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **File Management (Gestion des fichiers)**.

La boîte de dialogue File Management (Gestion des fichiers) apparaît.

- Le volet Folders (Dossiers) affiche les dossiers disponibles sur le disque.
- Le champ Flash Space (Espace flash) affiche la quantité totale de mémoire flash et la quantité de mémoire disponible.
- La zone Files (Fichiers) affiche les renseignements suivants sur les fichiers du dossier sélectionné :
  - Path
  - Filename
  - Taille (octets)
  - Heure de modification
  - Status (État), qui indique si un fichier sélectionné est désigné comme fichier de configuration de démarrage, fichier image de démarrage, fichier image ASDM, fichier image SVC, fichier image CSD ou fichier image APCF.

Étape 2 Cliquez sur **View** (Afficher) pour afficher le fichier sélectionné dans votre navigateur.

Étape 3 Cliquez sur **Cut** (Couper) pour couper le fichier sélectionné afin de le coller dans un autre répertoire.

Étape 4 Cliquez sur **Copy** (Copier) pour copier le fichier sélectionné afin de le coller dans un autre répertoire.

Étape 5 Cliquez sur **Paste** (Coller) pour coller le fichier copié dans la destination sélectionnée.

Étape 6 Cliquez sur **Delete** (Supprimer) pour supprimer le fichier sélectionné de la mémoire flash.

Étape 7 Cliquez sur **Rename** (Renommer) pour renommer un fichier.

Étape 8 Cliquez sur **New Directory** (Nouveau répertoire) pour créer un nouveau répertoire pour le stockage des fichiers.

Étape 9 Cliquez sur **File Transfer** (Transfert de fichiers) pour ouvrir la boîte de dialogue de transfert de fichiers. Consultez Transférer des fichiers, à la page 14 pour de plus amples renseignements.

Étape 10 Cliquez sur **Support Points** (Points de montage) pour ouvrir la boîte de dialogue Manage Mount Points (Gérer les points de montage). Consultez Ajouter des points de montage, à la page 12 pour de plus amples renseignements.

Transférer des fichiers

L'outil de transfert de fichiers vous permet de transférer des fichiers à partir d'un emplacement local ou distant. Vous pouvez transférer un fichier local sur votre ordinateur ou un système de fichiers flash vers et à partir de

l'ASA. Vous pouvez transférer un fichier distant vers et à partir de l'ASA en utilisant HTTP, HTTPS, TFTP, FTP ou SMB.

Remarque Pour le module logiciel IPS SSP, avant de télécharger le logiciel IPS sur disk0, assurez-vous qu'au moins 50 % de la mémoire flash est libre. Lorsque vous installez IPS, IPS réserve 50 % de la mémoire flash interne pour son système de fichiers.

Transférer des fichiers entre l'ordinateur local et la mémoire flash

Pour transférer des fichiers entre votre ordinateur local et un système de fichiers flash, procédez comme suit.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **File Management (Gestion des fichiers)**.

La boîte de dialogue File Management (Gestion des fichiers) apparaît.

Étape 2 Cliquez sur la flèche vers le bas à côté de **File Transfer** (Transfert de fichiers), puis cliquez sur **Between Local PC and Flash** (Entre l'ordinateur local et la mémoire flash).

La boîte de dialogue File Transfer (Transfert de fichiers) apparaît.

Étape 3 Sélectionnez et *faites glisser* le ou les fichiers depuis votre ordinateur local ou le système de fichiers flash que vous souhaitez charger ou télécharger vers l'emplacement souhaité. Vous pouvez également sélectionner les fichiers sur votre ordinateur local ou sur le système de fichiers flash que vous souhaitez charger ou télécharger, puis cliquer sur la flèche de droite ou de gauche pour transférer ces fichiers vers l'emplacement souhaité.

Étape 4 Cliquez sur **Close** (Fermer) lorsque vous avez terminé.

Transférer des fichiers entre le serveur distant et la mémoire flash

Pour transférer des fichiers entre un serveur distant et un système de fichiers flash, procédez comme suit.

Procédure

Étape 1 Dans la fenêtre d'application principale d'ASDM, choisissez **Tools (Outils)** > **File Management (Gestion des fichiers)**.

La boîte de dialogue File Management (Gestion des fichiers) apparaît.

Étape 2 Cliquez sur la flèche vers le bas dans la liste déroulante File Transfer (Transfert de fichiers), puis cliquez sur **Between Remote Server and Flash** (Entre le serveur distant et la mémoire flash).

La boîte de dialogue File Transfer (Transfert de fichiers) apparaît.

Étape 3 Pour transférer un fichier d'un serveur distant, cliquez sur l'option **Remote server** (Serveur distant).

Étape 4 Définissez le fichier source à transférer.

a) (Facultatif) Spécifiez l'interface par laquelle l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

b) Choisissez le chemin d'accès à l'emplacement du fichier, y compris l'adresse IP du serveur.



Remarque Le transfert de fichiers prend en charge les adresses IPv4 et IPv6.

c) Saisissez le type (si le chemin est FTP) ou le numéro de port (si le chemin est HTTP ou HTTPS) du serveur distant. Les types de FTP valides sont les suivants :

- ap : fichiers ASCII en mode passif
- an : fichiers ASCII en mode non passif
- ip : fichiers image binaires en mode passif
- in : fichiers image binaires en mode non passif

Étape 5 Pour transférer le fichier à partir du système de fichiers flash, cliquez sur l'option **Flash file system** (Système de fichiers flash).

Étape 6 Saisissez le chemin d'accès à l'emplacement du fichier ou cliquez sur **Browse Flash** (Parcourir la mémoire flash) pour trouver l'emplacement du fichier.

Étape 7 En outre, vous pouvez copier un fichier à partir de votre configuration de démarrage, de la configuration en cours d'exécution ou d'un système de fichiers SMB au moyen de l'interface de ligne de commande. Pour obtenir des instructions sur l'utilisation de la commande **copy**, consultez le guide de configuration de l'interface de ligne de commande.

Étape 8 Définissez la destination du fichier à transférer.

a) Pour transférer le fichier dans le système de fichiers flash, choisissez l'option **Flash file system** (Système de fichiers flash).

b) Saisissez le chemin d'accès à l'emplacement du fichier ou cliquez sur **Browse Flash** (Parcourir la mémoire flash) pour trouver l'emplacement du fichier.

Étape 9 Pour transférer un fichier vers un serveur distant, sélectionnez l'option **Remote server** (Serveur distant).

a) (Facultatif) Spécifiez l'interface par laquelle l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

b) Saisissez le chemin d'accès à l'emplacement du fichier.

c) Pour les transferts FTP, saisissez le type. Les types valides sont les suivants :

- ap : fichiers ASCII en mode passif
- an : fichiers ASCII en mode non passif
- ip : fichiers image binaires en mode passif
- in : fichiers image binaires en mode non passif

Étape 10 Cliquez sur **Transfer** (Transférer) pour commencer le transfert de fichiers.

La boîte de dialogue Enter Username and Password (Saisir le nom d'utilisateur et le mot de passe) apparaît.

Étape 11 Saisissez le nom d'utilisateur, le mot de passe et le domaine (si nécessaire) pour le serveur distant.

Étape 12 Cliquez sur **OK** pour continuer le transfert de fichiers.

Le processus de transfert de fichiers peut prendre quelques minutes; assurez-vous d'attendre la fin de l'opération.

Étape 13 Cliquez sur **Close** (Fermer) lorsque le transfert de fichiers est terminé.

Définir l'image ASA, ASDM et la configuration de démarrage

Si vous avez plus d'une image ASA ou ASDM, vous devez spécifier l'image que vous souhaitez démarrer. Si vous ne définissez pas l'image, l'image de démarrage par défaut est utilisée et cette image peut ne pas être celle prévue. Pour la configuration de démarrage, vous pouvez éventuellement spécifier un fichier dans le système de fichiers visible au lieu d'un répertoire masqué.

Voir les directives suivantes concernant les modèles :

- Châssis Firepower 4100/9300 : les mises à niveau ASA sont gérées par FXOS; vous ne pouvez pas mettre à niveau l'ASA dans le système d'exploitation de l'ASA, donc n'utilisez pas cette procédure pour l'image de l'ASA. Vous pouvez mettre à niveau ASA et FXOS séparément, car ils sont répertoriés séparément dans la liste du répertoire FXOS. L'ensemble ASA comprend toujours ASDM.
- Firepower 2100 en mode plateforme : les images ASA, ASDM et FXOS sont regroupées en un seul ensemble. Les mises à jour de paquets sont gérées par FXOS; vous ne pouvez pas mettre à niveau l'ASA dans le système d'exploitation de l'ASA, donc n'utilisez pas cette procédure pour l'image de l'ASA. Vous *ne pouvez pas* mettre à niveau ASA et FXOS séparément; ils sont toujours regroupés.
- Firepower 1000, 2100 en mode d'appareil, Secure Firewall 3100 : les images ASA, ASDM et FXOS sont regroupées en un seul paquet. Les mises à jour de paquets sont gérées par l'ASA à l'aide de cette procédure. Bien que ces plateformes utilisent l'ASA pour identifier l'image à démarrer, le mécanisme sous-jacent est différent de celui des ASA existants. Consultez la description de la commande ci-dessous pour plus d'informations.
- ASDM pour les modèles : ASDM peut être mis à niveau à partir du système d'exploitation de l'ASA, de sorte que vous n'avez pas besoin d'utiliser uniquement l'image ASDM fournie. Pour Firepower 2100 en mode plateforme et Firepower 4100/9300, les images ASDM que vous téléchargez manuellement ne s'affichent pas dans la liste d'images FXOS; vous devez les gérer à partir de l'ASA.



Remarque Lorsque vous mettez à niveau le paquet de l'ASA, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-782.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.

- ASA virtuel : le paquet de déploiement initial ASA virtuel place l'image de l'ASA dans la partition boot:/ en lecture seule. Lorsque vous mettez à niveau ASA virtuel, vous spécifiez une image différente dans la mémoire flash. Notez que si vous effacez votre configuration ultérieurement avec la commande, l' ASA virtuel reviendra au chargement de l'image de déploiement d'origine. Le paquet de déploiement initial ASA virtuel comprend également une image ASDM qu'il place dans la mémoire flash. Vous pouvez mettre à niveau l'image ASDM séparément.
- **disk0:** est la mémoire interne. D'autres numéros de lecteur représentent un stockage externe tel qu'un lecteur USB, un SSD ou une carte SD.

Consultez les paramètres par défaut suivants :

- Image ASA :
  - Firepower 1000, 2100 en mode d'appareil,1200/3100/4200 : démarre l'image de démarrage précédente.
  - ISA 3000 : démarre la première image d'application trouvée dans la mémoire flash interne.
  - ASA virtuel : démarre l'image dans la partition boot:/ en lecture seule qui a été créée lors du déploiement initial.
  - Châssis Firepower 4100/9300 : le système FXOS détermine quelle image ASA démarrer. Vous ne pouvez pas utiliser cette procédure pour définir l'image ASA.
  - Firepower 2100 en mode plateforme : le système FXOS détermine quel paquet ASA/FXOS démarrer. Vous ne pouvez pas utiliser cette procédure pour définir l'image ASA.
- Image ASDM sur tous les ASA : démarre la première image ASDM qu'il trouve dans la mémoire flash interne ou, si elle n'en existe pas à cet emplacement, dans la mémoire flash externe.
- Configuration de démarrage : par défaut, l'ASA démarre à partir d'une configuration de démarrage qui est un fichier masqué.

Procédure

Étape 1 Choisissez **Configuration** > **Management** > **System Image/Configuration** > **Boot Image/Configuration**.

Firepower 1000, 2100 en mode l'appareil, Secure : vous ne pouvez ajouter qu'une seule image. Si vous mettez à niveau vers une nouvelle image, vous devrez supprimer l'image précédente que vous avez définie. Lorsque vous appliquez ce changement, le système effectue une action : il valide et décompresse l'image et la copie dans l'emplacement de démarrage (un emplacement interne sur disk0 géré par FXOS). La nouvelle image sera chargée lorsque vous rechargerez l'ASA. Si vous changez d'avis avant de téléverser, vous pouvez supprimer **l'emplacement de l'image de démarrage** et soumettre une nouvelle demande pour supprimer la nouvelle image de l'emplacement de démarrage, de sorte que l'image actuelle continue de s'exécuter. Vous pouvez même supprimer le fichier image d'origine de la mémoire flash de l'ASA après avoir appliqué cette modification, et l'ASA démarrera correctement à partir de l'emplacement de démarrage. Contrairement à d'autres modèles, cette commande dans la configuration de démarrage n'affecte pas l'image de démarrage. La dernière image de démarrage chargée sera toujours exécutée lors du rechargement. Vous pouvez uniquement téléverser des images avec le nom de fichier d'origine à partir du site de téléchargement de Cisco. Si vous modifiez le nom de fichier, il ne se téléversera pas.

Autres modèles : vous pouvez spécifier jusqu'à quatre fichiers images binaires locaux à utiliser comme image de démarrage et une image sur un serveur TFTP à partir du périphérique de démarrage. Si vous spécifiez une image située sur un serveur TFTP, elle doit être la première de la liste. Si le périphérique ne peut pas atteindre le serveur TFTP pour téléverser l'image, il tente de téléverser le fichier image suivant de la liste située dans la mémoire flash.

Étape 2 Cliquez sur **Add** (Ajouter) dans le volet Boot Image/Configuration.

Étape 3 Accédez à l'image à partir de laquelle vous souhaitez démarrer. Pour une image TFTP, saisissez l'URL TFTP dans le champ File Name (nom de fichier). Cliquez sur **OK**.

Étape 4 Disposez les images dans l'ordre à l'aide des boutons de déplacement vers le haut et vers le bas.

Étape 5 (Facultatif) Dans le champ Boot Configuration File Path (chemin d'accès au fichier de configuration de démarrage), précisez le fichier de configuration de démarrage en cliquant sur **Browse Flash** (Parcourir la mémoire flash) et en sélectionnant la configuration. Cliquez sur **OK**.

Cette fonctionnalité est importante lorsque vous travaillez avec des configurations volumineuses qui ne tiennent pas dans le répertoire masqué. Si vous enregistrez une grande configuration et que vous voyez le message d'erreur suivant, veillez à enregistrer la configuration dans un nouveau fichier à l'aide de la commande suivante :

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

Étape 6 Dans le champ ASDM Image File Path (chemin d'accès au fichier image ASDM), précisez l'image ASDM en cliquant sur **Browse Flash** et en sélectionnant l'image. Cliquez sur **OK**.

Étape 7 Cliquez sur **Apply** (Appliquer).

Sauvegarde et restauration de configurations ou d'autres fichiers

Nous vous recommandons de faire des sauvegardes régulières de votre configuration et d'autres fichiers système pour éviter les défaillances du système.

Effectuer une sauvegarde ou une restauration complète du système

Ces procédures décrivent comment sauvegarder et restaurer les configurations et les images dans un fichier zip et le transférer sur votre ordinateur local.

Avant d'entreprendre la sauvegarde ou la restauration

- Vous devez avoir au moins 300 Mo d'espace disque disponible à l'emplacement de sauvegarde ou de restauration avant de lancer une sauvegarde ou une restauration.
- L'ASA doit être en mode de contexte unique.
- Vous ne pouvez lancer qu'une seule sauvegarde ou restauration à la fois.
- Si vous apportez des modifications à la configuration pendant ou après une sauvegarde, ces modifications ne seront pas incluses dans la sauvegarde. Si vous modifiez une configuration après avoir effectué la

sauvegarde, puis effectuez une restauration, cette modification de configuration sera remplacée. Par conséquent, l'ASA pourrait se comporter différemment.

- Ne remplacez pas ou ne restaurez pas le fichier de configuration système (*cspCfg.xml*) d'un ASA à un autre, en particulier entre les différents modèles de plateforme ASA. Le fichier *cspCfg.xml* peut contenir des informations sur le matériel propres au périphérique. La copie de ce fichier à partir d'un autre ASA peut créer une incompatibilité matérielle, telle que des différences dans le nombre de cœurs de CPU. Cette incompatibilité peut empêcher l'ASA cible de démarrer correctement et finir par le faire passer en mode Failsafe.
- Vous pouvez uniquement restaurer une configuration sur la même version ASA que celle lorsque vous avez effectué la sauvegarde d'origine. Vous ne pouvez pas utiliser l'outil de restauration pour migrer une configuration d'une version ASA vers une autre. Si une migration de configuration est requise, l'ASA met automatiquement à niveau la configuration de démarrage résidente lorsqu'il charge le nouveau système d'exploitation de l'ASA.
- Si vous utilisez la mise en grappe, vous pouvez uniquement sauvegarder ou restaurer les certificats de configuration de démarrage, de configuration d'exécution et d'identité. Vous devez créer et restaurer une sauvegarde séparément pour chaque unité.
- Si vous utilisez le basculement, vous devez créer et restaurer une sauvegarde séparément pour les unités actives et de secours.
- Si vous définissez une phrase secrète principale pour l'ASA, vous avez besoin de cette phrase secrète principale pour restaurer la configuration de sauvegarde que vous créez avec cette procédure. Si vous ne connaissez pas la phrase secrète principale pour l'ASA, consultez Configurer la phrase secrète principale pour savoir comment la réinitialiser avant de poursuivre la sauvegarde.
- Si vous importez des données PKCS12 (avec la commande **crypto ca trustpoint**) et que le point de confiance utilise des clés RSA, la paire de clés importée se voit attribuer le même nom que le point de confiance. En raison de cette limite, si vous spécifiez un nom différent pour le point de confiance et sa paire de clés après avoir restauré une configuration ASDM, la configuration de démarrage sera la même que la configuration d'origine, mais la configuration d'exécution comprendra un nom de paire de clés différent. Cela signifie que si vous utilisez des noms différents pour la paire de clés et le point de confiance, vous ne pouvez pas restaurer la configuration d'origine. Pour contourner ce problème, assurez-vous d'utiliser le même nom pour le point de confiance et sa paire de clés.
- Vous ne pouvez pas sauvegarder à l'aide de l'interface de ligne de commande et restaurer à l'aide d'ASDM, ou inversement.
- Chaque fichier de sauvegarde comprend le contenu suivant :
  - Configuration d'exécution
  - Configuration du démarrage
  - Toutes les images de sécurité

    Images de Cisco Secure Desktop et de l'analyse de l'hôte

    Paramètres de Cisco Secure Desktop et de l'analyse de l'hôte

    Images et profils (SVC) deSecure Client (services client sécurisés)

    Personnalisations et transformations (SVC) deSecure Client (services client sécurisés)
  - Certificats d'identité (inclut les paires de clés RSA liées aux certificats d'identité; exclut les clés autonomes)

- Clés prépartagées VPN
- Configurations SSL VPN
- Cadre personnalisé du profil d'application (APCF)
- Signets
- Personnalisations
- Politique d'accès dynamique (DAP)
- Modules d'extension
- Scripts de préremplissage pour les profils de connexion
- Configuration automatique du serveur mandataire
- Table de traduction
- Web content
- Information de version

Sauvegarder le système

Cette procédure décrit comment effectuer une sauvegarde complète du système.



Remarque Si le processus de sauvegarde se bloque, il est possible que votre ASDM ne dispose pas de suffisamment de mémoire pour charger la configuration. Vous pouvez superviser la console Java pour détecter le message « java.lang.OutOfMemoryError » afin de déterminer si le problème est lié à un manque de mémoire. Pour augmenter la mémoire ASDM, consultez Augmenter la mémoire de configuration de l'ASDM.

Procédure

Étape 1 Créez un dossier sur votre ordinateur pour stocker les fichiers de sauvegarde afin qu'ils soient faciles à trouver au cas où vous deviez les restaurer ultérieurement.

Étape 2 Choisissez **Tools (Outils)** > **Backup Configurations (Configurations de sauvegarde)**.

La boîte de dialogue Backup Configurations (Configurations de sauvegarde) s'affiche. Cliquez sur la flèche vers le bas dans la zone **SSL VPN Configuration** (Configuration SSL VPN) pour afficher les options de sauvegarde des configurations SSL VPN. Par défaut, tous les fichiers de configuration sont vérifiés et seront sauvegardés s'ils sont disponibles. Si vous souhaitez sauvegarder tous les fichiers de la liste, passez à l'étape 5.

Étape 3 Décochez la case **Backup All** (Sauvegarder tout) si vous souhaitez sélectionner les configurations à sauvegarder.

Étape 4 Cochez la case à côté de l'option que vous souhaitez sauvegarder.

Étape 5 Cliquez sur **Browse Local (Parcourir local) pour spécifier un répertoire et un nom de fichier pour le fichier de sauvegarde .zip.**

Étape 6 Dans la boîte de dialogue Select (Sélectionner), choisissez le répertoire dans lequel vous souhaitez stocker le fichier de sauvegarde.

Étape 7 Cliquez sur **Select** (sélectionner). Le chemin d'accès apparaît dans le champ Backup File (Fichier de sauvegarde).

Étape 8 Saisissez le nom du fichier de sauvegarde de destination après le chemin d'accès au répertoire. Le nom du fichier de sauvegarde doit comporter entre 3 et 232 caractères.

Étape 9 Cliquez sur **Backup** (Sauvegarde). La sauvegarde se poursuit immédiatement, sauf si vous sauvegardez des certificats ou que l'ASA utilise une phrase secrète principale.

Étape 10 Si vous avez configuré et activé une phrase secrète principale sur votre ASA, vous recevez un message d'avertissement avec une proposition de modification de la phrase secrète principale, si vous ne la connaissez pas, avant de procéder à la sauvegarde. Cliquez sur Yes (Oui) pour poursuivre la sauvegarde si vous connaissez la phrase secrète principale. La sauvegarde se poursuit immédiatement, sauf si vous sauvegardez des certificats d'identité.

Étape 11 Si vous sauvegardez un certificat d'identité, vous devez saisir une phrase secrète distincte à utiliser pour le chiffrement des certificats au format PKCS12. Vous pouvez saisir une phrase secrète ou ignorer cette étape.



Remarque Seuls les certificats d'identité sont sauvegardés par ce processus.

- Pour chiffrer les certificats, saisissez et confirmez votre phrase secrète dans la boîte de dialogue Certificate Passphrase (Phrase secrète du certificat) et cliquez sur OK. Vous devrez vous souvenir du mot de passe que vous avez saisi dans cette boîte de dialogue lors de la restauration des certificats.
- Cliquez sur **Cancel** (Annuler) pour ignorer cette étape et ne pas sauvegarder les certificats.

Après avoir cliqué sur OK ou Cancel (Annuler), la sauvegarde commence immédiatement.

Étape 12 Une fois la sauvegarde terminée, la fenêtre d'état se ferme et la boîte de dialogue Backup Statistics (Statistiques de sauvegarde) apparaît pour afficher des messages de réussite et d'échec.



Remarque Les « messages d'échec » des sauvegardes sont très probablement causés par l'absence de configuration existante pour les types indiqués.

Étape 13 Cliquez sur **OK** pour fermer la boîte de dialogue Backup Statistics (Statistiques de sauvegarde).

Restaurer la sauvegarde

Vous pouvez spécifier les configurations et les images à restaurer à partir d'un fichier zip tar.gz sur votre ordinateur local.



Remarque Si le processus de restauration se bloque, il est possible que votre ASDM ne dispose pas de suffisamment de mémoire pour charger la configuration. Vous pouvez superviser la console Java pour détecter le message « java.lang.OutOfMemoryError » afin de déterminer si le problème est lié à un manque de mémoire. Pour augmenter la mémoire ASDM, consultez Augmenter la mémoire de configuration de l'ASDM.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Restore Configurations (Restaurer les configurations)**.

Étape 2 Dans la boîte de dialogue Restore Configurations (Restaurer les configurations), cliquez sur **Browse Local Directory** (Parcourir le répertoire local), choisissez le fichier zip sur votre ordinateur local qui contient la configuration à restaurer, puis cliquez sur **Select** (Sélectionner). Le chemin d'accès et le nom du fichier zip apparaissent dans le champ **Local File** (Fichier local).

Le fichier zip que vous restaurez doit être créé en sélectionnant l'option **Tools (Outils) > Backup Configurations (Configurations de sauvegarde)**.

Étape 3 Cliquez sur **Next** (suivant). La boîte de dialogue Restore Configurations (Restaurer les configurations) s'affiche. Cochez les cases en regard des configurations que vous souhaitez restaurer. Toutes les configurations SSL VPN disponibles sont sélectionnées par défaut.

Étape 4 Cliquez sur **Restaurer**.

Étape 5 Si vous avez spécifié une phrase secrète pour chiffrer les certificats lors de la création du fichier de sauvegarde, ASDM vous invite à saisir cette phrase secrète.

Étape 6 Si vous avez choisi de restaurer la configuration en cours d'exécution, il vous est demandé si vous souhaitez fusionner la configuration en cours d'exécution, remplacer la configuration en cours d'exécution ou ignorer cette partie du processus de restauration.

- La fusion des configurations combine la configuration en cours d'exécution actuelle et la configuration en cours d'exécution sauvegardée.
- Le remplacement de la configuration en cours d'exécution utilise uniquement la configuration en cours d'exécution sauvegardée.
- Ignorer cette étape ne restaure pas la configuration en cours d'exécution sauvegardée.

ASDM affiche une boîte de dialogue d'état jusqu'à ce que l'opération de restauration soit terminée.

Étape 7 Si vous avez remplacé ou fusionné la configuration en cours d'exécution, fermez ASDM et redémarrez-le. Si vous n'avez pas restauré la configuration en cours d'exécution, actualisez la session ASDM pour que les modifications prennent effet.

Configurer la sauvegarde et la restauration automatiques (ISA 3000)

Sur l'ISA 3000, vous pouvez configurer des sauvegardes automatiques vers un emplacement particulier chaque fois que vous enregistrez votre configuration.

La restauration automatique vous permet de configurer facilement de nouveaux périphériques avec une configuration complète chargée sur une carte de mémoire flash SD. La restauration automatique est activée dans la configuration d'usine par défaut.

Configurer la sauvegarde automatique (ISA 3000)

Sur l'ISA 3000, vous pouvez configurer des sauvegardes automatiques vers un emplacement particulier chaque fois que vous enregistrez votre configuration.

Avant de commencer

Cette fonctionnalité est uniquement disponible sur l'ISA 3000.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Auto Backup and Restore Configuration (Configuration de la sauvegarde et de la restauration automatiques)**.

Étape 2 Cochez ou décochez la case **Automate Backup Configuration** (Automatiser la configuration de la sauvegarde) pour activer ou désactiver les sauvegardes automatiques.

Si vous activez les sauvegardes automatiques, lorsque vous enregistrez la configuration, la configuration est automatiquement enregistrée à l'emplacement de sauvegarde ainsi que dans la configuration de démarrage. Le fichier de sauvegarde est intitulé « auto-backup-asa.tgz ».

Définissez les paramètres suivants :

- **Interface** : spécifie l'interface permettant d'atteindre l'URL de sauvegarde, si vous spécifiez un stockage hors périphérique. Si vous ne spécifiez pas de nom d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.
- **Location** (Emplacement) : spécifie le support de stockage à utiliser pour la sauvegarde des données. Vous pouvez définir une URL ou un stockage local. disk0 est le lecteur flash interne, disk1 est une clé de mémoire USB facultative sur USB 1 et disk2 est une clé de mémoire USB facultative sur USB 2. Et disk3 est la carte mémoire SD. La valeur par défaut pour la restauration automatique est disk3.
- **Passphrase** (Phase secrète) : définit la phrase secrète pour sécuriser les données sauvegardées. La valeur par défaut pour la restauration automatique est « cisco ».

Configurer la restauration automatique (ISA 3000)

Le mode de restauration automatique restaure la configuration système sur un périphérique sans intervention de l'utilisateur. Par exemple, vous insérez une carte de mémoire SD contenant une configuration de sauvegarde enregistrée dans un nouveau périphérique, puis mettez celui-ci sous tension. Lorsque le périphérique se manifeste, il vérifie la carte SD pour décider si la configuration système doit être restaurée. (La restauration n'est lancée que si le fichier de sauvegarde comporte l'« empreinte digitale » d'un autre périphérique. L'empreinte du fichier de sauvegarde est mise à jour pour correspondre au périphérique actuel lors d'une opération de sauvegarde ou de restauration. Donc, si le périphérique a déjà effectué une restauration ou s'il a créé sa propre sauvegarde, la restauration automatique est ignorée.) Si l'empreinte indique qu'une restauration est requise, le périphérique remplace la configuration système (startup-config, running-config, configuration du SSL VPN, etc.; consultez Sauvegarder le système, à la page 21 pour plus de détails sur le contenu de la sauvegarde). Lorsque le périphérique a terminé son démarrage, il exécute la configuration enregistrée.

La restauration automatique est activée dans la configuration d'usine par défaut. Vous pouvez donc facilement configurer de nouveaux périphériques avec une configuration complète chargée sur une carte de mémoire SD sans avoir à effectuer de préconfiguration du périphérique.

Étant donné que le périphérique doit décider dès le début du processus de démarrage si la configuration système doit être restaurée, il vérifie les variables ROMMON pour déterminer si le périphérique est en mode de restauration automatique et pour obtenir l'emplacement de la configuration de sauvegarde. Les variables ROMMON suivantes sont utilisées :

- **RESTORE_MODE =** {**auto** | **manual**}

  La valeur par défaut est **auto**.

- **RESTORE_LOCATION =** {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  La valeur par défaut est **disk3:**.

- **RESTORE_PASSPHRASE** = *key*

  La valeur par défaut est **cisco**.

Pour modifier les paramètres de restauration automatique, procédez comme suit.

Avant de commencer

- Cette fonctionnalité est uniquement disponible sur l'ISA 3000.
- Si vous utilisez les paramètres de restauration par défaut, une carte de mémoire SD doit être installée (numéro de pièce SD-IE-1GB=).
- Si vous devez restaurer la configuration par défaut pour vous assurer que la restauration automatique est activée, utilisez la commande **configure factory default**. Cette commande est uniquement disponible en mode de pare-feu transparent. Par conséquent, si vous êtes en mode de pare-feu routé, utilisez d'abord la commande **firewall transparent**.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Auto Backup and Restore Configuration (Configuration de la sauvegarde et de la restauration automatiques)**.

Étape 2 Cochez ou décochez la case **Automate Restore Configuration** (Automatiser la configuration de la restauration) pour activer ou désactiver la restauration automatique.

Le nom du fichier restauré est « auto-backup-asa.tgz ». Si vous activez la restauration automatique, définissez les paramètres suivants :

- **Location** (Emplacement) : spécifie le support de stockage à utiliser pour la restauration des données. disk0 est le lecteur flash interne, disk1 est une clé de mémoire USB facultative sur USB 1 et disk2 est une clé de mémoire USB facultative sur USB 2. Et disk3 est la carte mémoire SD. La valeur par défaut est disk3.
- **Passphrase** (Phase secrète) : définit la phrase secrète pour lire les données sauvegardées. La valeur par défaut est « cisco ».

Enregistrer la configuration en cours d'exécution sur un serveur TFTP

Cette fonctionnalité stocke une copie du fichier de configuration en cours d'exécution sur un serveur TFTP.

Procédure

Étape 1 Choisissez **File (Fichier)** > **Save Running Configuration to TFTP Server (Enregistrer la configuration en cours d'exécution sur un serveur TFTP)**.

La boîte de dialogue Save Running Configuration to TFTP Server (Enregistrer la configuration en cours d'exécution sur le serveur TFTP) s'affiche.

Étape 2 Saisissez l'adresse IP du serveur TFTP et le chemin d'accès au fichier sur le serveur TFTP dans lequel le fichier de configuration sera enregistré, puis cliquez sur **Save Configuration** (Enregistrer la configuration).

Remarque Pour configurer les paramètres TFTP par défaut, choisissez **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > TFTP Client (Client TFTP)**. Après avoir configuré ce paramètre, l'adresse IP du serveur TFTP et le chemin d'accès au fichier sur le serveur TFTP s'affichent automatiquement dans cette boîte de dialogue.

Programmer un redémarrage du système

L'outil System Reload (Rechargement du système) vous permet de planifier le redémarrage du système ou d'annuler un redémarrage en attente.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **System Reload (Rechargement du système)**.

Étape 2 Dans la zone Reload Scheduling (Planification du rechargement), définissez les paramètres suivants :

a) Pour l'état de configuration, choisissez d'enregistrer ou de supprimer la configuration en cous d'exécution au redémarrage.

b) Pour l'heure de début du rechargement, choisissez parmi les options suivantes :

- Cliquez sur **Now** (Maintenant) pour effectuer un redémarrage immédiat.
- Cliquez sur **Delay by** (Retarder de) pour retarder le redémarrage d'une durée spécifiée. Saisissez le temps avant que le redémarrage ne commence, en heures et en minutes ou en minutes seulement.
- Cliquez sur **Schedule at** (Planifier à) pour planifier le redémarrage à une heure et à une date précises. Saisissez l'heure du jour à laquelle le redémarrage doit se produire et sélectionnez la date du redémarrage planifié.

c) Dans le champ Reload Message (Recharger le message), saisissez un message à envoyer aux instances ouvertes d'ASDM au redémarrage.

d) Cochez la case **On reload failure force immediate reload after** (En cas d'échec du rechargement, forcer un rechargement immédiat après) pour afficher le temps écoulé en heures et en minutes ou seulement en minutes avant de retenter un redémarrage.
e) Cliquez sur **Schedule Reload** (Planifier le rechargement) pour planifier le redémarrage comme configuré.

La zone Reload Status (État du rechargement) affiche l'état du redémarrage.

Étape 3 Effectuez l'une des opérations suivantes :

- Cliquez sur **Cancel Reload** (Annuler le rechargement) pour arrêter un redémarrage planifié.
- Cliquez sur **Refresh** (Actualiser) pour actualiser l'affichage de l'état du rechargement une fois le redémarrage planifié terminé.
- Cliquez sur **Details** (Détails) pour afficher les résultats d'un redémarrage planifié.

Échange à chaud d'un SSD sur Cisco Secure Firewall

Si vous avez deux disques SSD, ils forment un RAID lorsque vous démarrez. Vous pouvez effectuer les tâches suivantes au niveau de l'interface de ligne de commande lorsque le pare-feu est sous tension :

- Échangez à chaud un des disques SSD : si un disque SSD est défectueux, vous pouvez le remplacer. Notez que si vous n'avez qu'un seul disque SSD, vous ne pouvez pas le retirer tant que le pare-feu est sous tension.
- Retirez un des disques SSD : si vous avez deux disques SSD, vous pouvez en retirer un.
- Ajouter un deuxième SSD : si vous avez un deuxième SSD, vous pouvez en ajouter un deuxième et former un RAID.

  Lorsque vous utilisez un seul disque SSD dans les périphériques Secure Firewall, l' **état du disque** indiquera **détérioré**.



Mise en garde Ne retirez pas physiquement un SSD sans l'avoir supprimé du RAID en suivant cette procédure. Vous pourriez entraîner des pertes de données.

Procédure

Étape 1 Retirez l'un des disques SSD.

a) Retirez le SSD du RAID.

raid remove-secure local-disk {**1** | **2**}

Le mot clé **remove-secure** supprime le SSD du RAID, désactive la fonction de disque à chiffrement automatique et effectue un effacement sécurisé du SSD. Si vous souhaitez uniquement retirer le SSD du RAID et conserver les données intègres, vous pouvez utiliser le mot clé **remove**.

Exemple :

```
ciscoasa(config)# raid remove-secure local-disk 2
```

b) Surveiller l'état RAID jusqu'à ce que SSD ne s'affiche plus dans l'inventaire.

show raid

Une fois le SSD retiré du RAID, l'**exploitabilité** et **l'état du lecteur** s'affichent comme **dégradés**. Le deuxième lecteur ne sera plus répertorié en tant que disque membre.

Exemple :

```
ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
```

```
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) Retirez physiquement le disque SSD du châssis.

Étape 2 Ajouter un disque SSD.

a) Ajoutez physiquement le SSD dans le logement vide.

b) Ajoutez le SSD au RAID.

raid add local-disk {**1** | **2**}

La synchronisation du nouveau SSD avec le RAID peut prendre plusieurs heures, pendant laquelle le pare-feu est complètement opérationnel. Vous pouvez même redémarrer et la synchronisation se poursuivra après la mise sous tension. Utilisez la commande **show raid** pour afficher l'état.

Si vous installez un disque SSD qui a été utilisé précédemment sur un autre système et qui est toujours verrouillé, saisissez la commande suivante :

raid add local-disk {**1** | **2**} *psid*

Le *psid* est imprimé sur l'étiquette fixée à l'arrière du disque SSD. Sinon, vous pouvez redémarrer le système et le SSD sera formaté et ajouté au RAID.

Historique des logiciels et des configurations

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Client et serveur Secure Copy	9.1(5)/9.2(1)	L'ASA prend désormais en charge le client et le serveur Secure Copy (SCP) pour transférer des fichiers vers et depuis un serveur SCP. Nous avons modifié les écrans suivants : Tools (Outils) > File Management (Gestion des fichiers) > File Transfer (Transfert de fichiers) > Between Remote Server and Flash (Entre le serveur distant et la configuration flash) **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès aux fichiers) > Secure Copy (SCP) Server (Serveur Secure Copy (SCP))**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Chiffrement SSH et d'intégrité configurables	9.1(7)/9.4(3)/9.5(3)/9.6(1)	Les utilisateurs peuvent sélectionner des modes de chiffrement lors de la gestion du chiffrement SSH et peuvent configurer le HMAC et le chiffrement pour divers algorithmes d'échange de clés. Vous souhaiterez peut-être modifier les chiffres pour qu'ils soient plus ou moins stricts, selon votre application. Notez que la performance de la copie sécurisée dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier les chiffres proposés, utilisez **ssh cipher encryption custom aes128-cbc**, par exemple. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffres SSH)**
Vérification du certificat du serveur de mise à jour automatique activée par défaut	9.2(1)	La vérification du certificat du serveur de mise à jour automatique est maintenant activée par défaut; pour les nouvelles configurations, vous devez explicitement désactiver la vérification de certificat. Si vous effectuez une mise à niveau à partir d'une version antérieure et que vous n'avez pas activé la vérification de certificat, la vérification de certificat n'est pas activée, et l'avertissement suivant s'affiche : `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` La configuration sera migrée vers la configuration explicite sans vérification. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > System/Image Configuration (Configuration système/image) > Auto Update (Mise à jour automatique) > Add Auto Update Server (Ajouter l'Auto Update Server).
Sauvegarde et restauration du système à l'aide de l'interface de ligne de commande	9.3(2)	Vous pouvez maintenant sauvegarder et restaurer des configurations système complètes, y compris les images et les certificats, à l'aide de l'interface de ligne de commande. Nous n'avons pas modifié d'écrans ASDM.
Récupération et chargement d'une nouvelle image ASA 5506W-X	9.4(1)	Nous prenons désormais en charge la récupération et le chargement d'une nouvelle image ASA 5506W-X. Nous n'avons pas modifié d'écrans ASDM.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Sauvegarde et restauration automatiques pour l'ISA 3000	9.7(1)	Vous pouvez activer la fonction de sauvegarde automatique et/ou de restauration automatique en utilisant les paramètres prédéfinis dans les commandes de sauvegarde et de restauration. Les scénarios de ces fonctionnalités comprennent la configuration initiale à partir d'un support externe; le remplacement de l'appareil; la restauration à un état opérationnel. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Auto Backup and Restore Configuration (Configuration de la sauvegarde et de la restauration automatiques)**
La pile CiscoSSH requiert un accès SSH lors de l'utilisation du client SCP	9.17(1)	Si vous utilisez la pile CiscoSSH, ou utilisez la commande ASA **copy** de l'ASA pour copier un fichier vers ou à partir d'un serveur SCP, vous devez activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP
Prise en charge RAID pour les SSD sur le pare-feu Secure Firewall 3100	9.17(1)	Les disques SSD sont des disques à chiffrement automatique (SED), et si vous avez deux disques SSD, ils forment un RAID logiciel. Commandes nouvelles ou modifiées : **raid, show raid, show ssd**

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.