Logiciels et configurations

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

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. Consultez les problèmes connus suivants relatifs à la rétrogradation. Veuillez noter que d'autres problèmes peuvent vous obliger à recharger vos unités de grappe, ce qui entraînera un temps d'arrêt.

- **La rétrogradation à une version antérieure à la version 9.9(1) avec mise en grappe**: la version 9.9(1) et les versions ultérieures inclut une amélioration de la distribution des sauvegardes. Si vous avez au moins 3 unités dans la grappe, vous devez effectuer les étapes suivantes :

  1. Supprimez toutes les unités secondaires de la grappe (pour que celle-ci ne se compose que de l'unité principale).
  2. Rétrogradez une unité secondaire et réintégrez-la à la grappe.
  3. Désactivez la mise en grappe sur l'unité principale, rétrogradez-la et réintégrez-la à la grappe.
  4. Rétrogradez les unités secondaires restantes et joignez-les à la grappe, une à la fois.

- **Rétrograder à une version antérieure à la version 9.9(1) lorsque vous activez la redondance du site en grappe** : vous devez désactiver la redondance de site si vous souhaitez effectuer une rétrogradation (ou si vous souhaitez ajouter à une grappe une unité dont la version est antérieure à la version 9.9(1)). Sinon, vous constaterez des effets secondaires, par exemple des flux de transfert fictifs sur l'unité exécutant l'ancienne version.
- **Rétrogradation à partir de la version 9.8(1) avec mise en grappe et carte de chiffrement** : il n'y a pas de prise en charge de la rétrogradation sans temps d'arrêt à partir de la version 9.8(1) lorsqu'une carte de chiffrement est configurée. Vous devez effacer la configuration de la carte de chiffrement avant la rétrogradation, puis réappliquer la configuration après la rétrogradation.
- **Rétrograder de la version 9.8(1) avec un contrôle d'intégrité de l'unité de mise en grappe défini sur 0,3 à 0,7 seconde** : si vous rétrogradez votre logiciel ASA après avoir défini le délai de rétention sur 0,3–0,7 (**health-check holdtime**), ce paramètre reviendra à la valeur par défaut de 3 secondes, car le nouveau paramètre n'est pas pris en charge.
- **Rétrogradation à partir de la version 9.5(2) ou d'une version ultérieure à la version 9.5(1) ou une version antérieure avec mise en grappe (CSCuv82933) :** il n'y a pas de prise en charge de la rétrogradation sans temps d'arrêt à partir de la version 9.5(2). Vous devez recharger toutes les unités à peu près en même temps afin qu'un nouveau cluster se forme lorsque les unités sont de nouveau en ligne. Si vous attendez pour recharger les unités de manière séquentielle, elles ne pourront pas former de grappe.
- **Rétrogradation à partir de la version 9.2(1) ou d'une version ultérieure à la version 9.1 ou une version antérieure avec mise en grappe** : la rétrogradation sans temps d'arrêt n'est pas prise en charge.

- **Problème de rétrogradation de la version 9.18 ou ultérieure** : il y a un changement de comportement dans la version 9.18 où la commande **access-group** sera répertoriée avant ses commandes **access-list**. Si vous effectuez une rétrogradation, la commande **access-group** sera rejetée, car elle n'a pas encore chargé les commandes **access-list**. Ce résultat se produit même si vous avez précédemment activé la commande **forward-reference enable**, car cette commande est maintenant supprimée. Avant de procéder à la rétrogradation, assurez-vous de copier toutes les commandes **access-group** manuellement, puis après la rétrogradation, saisissez-les de nouveau.
- **Problème de rétrogradation du Firepower 2100 en mode plateforme à partir de la version 9.13/9.14 à la version 9.12 ou à une version antérieure** : pour un Firepower 2100 disposant d'une nouvelle installation de la version 9.13 ou 9.14 que vous avez convertie en mode plateforme : si vous rétrogradez le périphérique à la version 9.12 ou à une version antérieure, vous ne pourrez pas configurer de nouvelles interfaces ni modifier des interfaces existantes dans FXOS (notez que la version 9.12 et les versions antérieures ne prennent en charge que le mode plateforme). Vous devez soit restaurer votre version à la

version 9.13 ou à une version ultérieure, soit effacer votre configuration à l'aide de la commande de configuration d'effacement FXOS. Ce problème ne se produit pas si vous avez initialement effectué une mise à niveau vers la version 9.13 ou 9.14 à partir d'une version antérieure. Seules les nouvelles installations sont concernées, comme un nouveau périphérique ou un périphérique recréé. (CSCvr19755)

- **Rétrogradation de la version 9.10(1) pour les licences Smart** : en raison de modifications dans l'agent Smart, si vous effectuez une rétrogradation, vous devez réenregistrer votre périphérique auprès de Cisco Smart Software Manager. Le nouvel agent Smart utilise un fichier chiffré. Vous devez donc vous réenregistrer pour utiliser un fichier non chiffré requis par l'ancien agent Smart.
- **Rétrograder à la version 9.5 ou à une version antérieure avec des mots de passe utilisant le hachage PBCDF2 (Password-Based Key Derivation Function 2)** : les versions antérieures à la version 9.6 ne prennent pas en charge le hachage PBKDF2. Dans la version 9.6(1), les mots de passe **enable** et **username** de plus de 32 caractères utilisent le hachage PBCDF2. Dans la version 9.7(1), les nouveaux mots de passe de toutes les longueurs utilisent le hachage PBCDF2 (les mots de passe existants continuent d'utiliser le hachage MD5). Si vous effectuez une rétrogradation, le mot de passe de **enable** revient à la valeur par défaut (c'est-à-dire vide). Les noms d'utilisateur ne seront pas analysés correctement, et les commandes **username** seront supprimées. Vous devez recréer vos utilisateurs locaux.
- **Rétrograder à partir de la version 9.5(2.200) pour le ASA virtuel** : le ASA virtuel ne conserve pas l'état d'enregistrement de la licence. Vous devez vous réenregistrer à l'aide de la commande **license smart register idtoken id_token force** (pour ASDM : consultez la page **Configuration > Device Management (Gestion des périphériques) > Licensing (Licences) > Smart Licensing (Licences Smart)** et utilisez l'option **Force registration** (Forcer l'enregistrement)); obtenez le jeton d'identification auprès de Smart Software Manager.
- **Les tunnels VPN sont répliqués sur l'unité de secours même si cette dernière exécute une version du logiciel qui ne prend pas en charge la suite de chiffrement que le tunnel d'origine a négociée.** Ce scénario se produit lors de la rétrogradation. Dans ce cas, déconnectez votre connexion VPN et reconnectez-vous.

Configuration incompatible supprimée après la rétrogradation

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

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

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

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

rétrogradez le logiciel et restaurez l'ancienne configuration.

downgrade [**/noconfirm**] *ancienne_url_d_image ancienne_url_de_configuration* [**activation-key** *ancienne_clé*]

Exemple :

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

L'option **/noconfirm** est rétrogradée sans invite. L'*url_de_l_image* est le chemin d'accès à l'ancienne image sur disk0, disk1, tftp, ftp ou smb. L'*ancienne_url_de_configuration* est le chemin d'accès à la configuration de pré-migration enregistrée. Si vous devez revenir à une clé d'activation antérieure à la version 8.3, vous pouvez saisir l'ancienne clé d'activation.

Gérer les fichiers

Afficher les fichiers dans la mémoire flash

Vous pouvez afficher les fichiers dans la mémoire flash et voir des renseignements sur les fichiers.

Procédure

Étape 1 Affichez les fichiers dans la mémoire flash :

dir [**disk***n***:**]

disk0: est la mémoire interne. D'autres numéros de lecteur représentent un stockage externe tel qu'un lecteur USB, un SSD ou une carte SD.

Exemple :

```
hostname# dir

Directory of disk0:/
500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
```

Étape 2 Affichez des renseignements étendus sur un fichier en particulier :

show file information [path:/]*filename*

Exemple :

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

La taille de fichier répertoriée est à titre d'exemple uniquement.

Le chemin par défaut est le répertoire racine de la mémoire flash interne (disk0:/).

Supprimer des fichiers de la mémoire flash

Vous pouvez supprimer des fichiers de la mémoire flash dont vous n'avez plus besoin.

Procédure

Supprimez un fichier de la mémoire flash :

delete disk*n***:** *filename*

disk0: est la mémoire interne. D'autres numéros de lecteur représentent un stockage externe tel qu'un lecteur USB, un SSD ou une carte SD.

Par défaut, le fichier est supprimé du répertoire de travail actuel si vous ne spécifiez pas de chemin. Vous pouvez utiliser des caractères génériques lors de la suppression de fichiers. Vous êtes invité à indiquer le nom de fichier à supprimer, puis vous devez confirmer la suppression.

Effacer le système de fichiers flash

Pour effacer le système de fichiers flash, procédez comme suit.

Procédure

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

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

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

Étape 4 Saisissez la commande **erase**, qui remplace tous les fichiers et efface le système de fichiers, y compris les fichiers système masqués :

rommon #1> **erase** [**disk0:** | **disk***n***:** | **usb:**]

disk0: est la mémoire interne. Les autres numéros de lecteur représentent le stockage externe. Les modèles plus récents utilisent **usb:** pour le lecteur USB externe.

Configurer l'accès au fichier

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

Configurer le mode client FTP

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

Procédure

Définissez le mode FTP sur passif :

ftp mode passive

Exemple :

```
ciscoasa(config)# ftp mode passive
```

Configurer l'ASA Secure Copy Client

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

La performance de SCP dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier le chiffrement proposé, utilisez la commande **ssh cipher encryption** le volet; par exemple, **ssh cipher encryption custom aes128-cbc**

Avant de commencer

- La licence ASA doit avoir la licence de cryptage renforcé (3DES/AES) pour prendre en charge les connexions SSH version 2.
- Sauf indication contraire, pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.
- Pour le serveur SCP, activez SSH sur l'ASA conformément à Configurer l'accès SSH.

Procédure

Étape 1 (Facultatif) L'ASA stocke la clé d'hôte SSH pour chaque serveur SCP auquel elle se connecte. Vous pouvez gérer manuellement les clés si vous le souhaitez.

ssh pubkey-chain [**no**] **server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*}

Exemple :

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:
e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12
```

Pour chaque serveur, vous pouvez spécifier la **key-string** (clé publique) ou le **key-hash** (valeur de hachage) de l'hôte SSH.

La *key_string* est la clé publique RSA codée en Base64 de l'homologue distant. Vous pouvez obtenir la valeur de clé publique à partir d'un client SSH ouvert; c'est-à-dire du fichier .ssh/id_rsa.pub. Après avoir soumis la clé publique codée en Base64, cette clé est ensuite hachée au moyen de SHA-256.

Le **key-hash** {**md5** | **sha256**} *fingerprint* saisit la clé déjà hachée (à l'aide d'une clé MD5 ou SHA-256); par exemple, une clé que vous avez copiée à partir de la sortie de la commande **show**.

Étape 2 (Facultatif) Activez ou désactivez la vérification de la clé d'hôte SSH. Pour le mode de contexte multiple, saisissez cette commande dans le contexte d'administration.

[**no**] **ssh stricthostkeycheck**

Exemple :

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

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

Exemples

L'exemple suivant ajoute une clé d'hôte déjà hachée pour le serveur à l'adresse 10.86.94.170 :

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:
64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

L'exemple suivant ajoute une clé de chaîne d'hôte pour le serveur à l'adresse 10.7.8.9 :

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:
46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

Configurer le chemin du client TFTP pour l'ASA

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

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

Procédure

Prédéfinissez l'adresse du serveur TFTP et le nom de fichier à utiliser avec les commandes **configure net** et **copy** :

tftp-server *interface_name server_ip filename*

Exemple :

```
ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg
ciscoasa(config)# copy tftp: test.cfg

Address or name of remote host [10.1.4.7]?

Source filename [files/config1.cfg]?config2.cfg

Destination filename [test.cfg]?

Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...
```

Vous pouvez remplacer le nom de fichier lorsque vous saisissez la commande; par exemple, lorsque vous utilisez la commande **copy**, vous pouvez tirer parti de l'adresse du serveur TFTP prédéfinie, mais saisir un nom de fichier dans les invites interactives.

Pour la commande **copy**, saisissez **tftp:** pour utiliser la valeur tftp-server au lieu de **tftp://***url*.

Copier un fichier sur l'ASA

Cette section décrit comment copier l'image de l'application, le logiciel ASDM, un fichier de configuration ou tout autre fichier qui doit être téléchargé dans la mémoire flash interne ou externe à partir d'un serveur TFTP, FTP, SMB, HTTP, HTTPS, SCP ou d'un lecteur tel qu'une clé USB.

Directives

- **disk0:** est la mémoire interne. D'autres numéros de lecteur représentent un stockage externe tel qu'un lecteur USB, un SSD ou une carte SD.
- Assurez-vous que le lecteur USB est au format EXT2/3/4 ou VFAT/FAT32.
- Vous ne pouvez pas avoir deux fichiers du même nom, mais avec une casse différente dans le même répertoire de mémoire flash. Par exemple, si vous tentez de télécharger le fichier Config.cfg à un emplacement qui contient le fichier config.cfg, vous recevez le message d'erreur suivant :

```
%Error opening disk0:/Config.cfg (File exists)
```

- Pour le mode de contexte multiple, vous devez être dans l'espace d'exécution du système, sauf si vous configurez le stockage privé (**storage-url private**). Dans un contexte, vous pouvez également copier la configuration de démarrage (voir Copier un fichier dans la configuration de démarrage ou d'exécution, à la page 18 si vous avez un stockage privé et Sauvegarder une configuration de contexte dans un contexte, à la page 33), ou une capture. SCP n'est pas pris en charge dans un contexte utilisant la pile CiscoSSH.

Avant de commencer

- Pour utiliser la commande **copy** de l'ASA afin de copier un fichier vers ou depuis un serveur SCP, vous devez :
  - (Pile CiscoSSH uniquement) Activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP à l'aide de la commande **ssh**.
  - Générer une paire de clés (pour les ASA physiques uniquement) à l'aide de la commande **crypto key generate**.

Procédure

Copiez un fichier en utilisant l'un des types de serveur suivants.

- Copiez à partir d'un serveur TFTP :

  copy [**/noconfirm**] [*interface_name*] **tftp:**//*server*[/*path*]/*src_filename* **disk***n***:**/[*path*/]*dest_filename*

  Exemple :

```
ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg

Address or name of remote host [10.1.1.67]?

Source filename [files/context1.cfg]?

Destination filename [context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- Copiez à partir d'un serveur FTP :

  copy [**/noconfirm**] [*interface_name*] **ftp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*src_filename* **disk***n***:**/[*path*/]*dest_filename*

  Exemple :

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg
disk0:/contexts/context1.cfg

Address or name of remote host [10.1.1.67]?

Source username [jcrichton]?
```

```
Source password [aeryn]?

Source filename [files/context1.cfg]?

Destination filename [contexts/context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- Copiez à partir d'un serveur HTTP(S) :

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  Exemple :

```
ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg

Address or name of remote host [10.1.1.67]?

Source username [asun]?

Source password [john]?

Source filename [files/moya.cfg]?

Destination filename [contexts/moya.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- Copiez à partir d'un serveur SMB :

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  Exemple :

```
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- Copiez à partir d'un serveur SCP :

  L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur SCP.

  copy [**/noconfirm**] [*interface_name*]
  scp://[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] **disk***n***:/**[*path/*]*dest_filename*

  Exemple :

```
ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg

Address or name of remote host [10.86.94.170]?
```

```
Source username [pilot]?

Destination filename [test.cfg]?

The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established.
RSA key fingerprint is
<65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19>(SHA256).
Are you sure you want to continue connecting (yes/no)? yes

Please use the following commands to add the hash key to the configuration:
  ssh pubkey-chain
    server 10.86.94.170
      key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19


Password: <type in password>
!!!!!!
6006 bytes copied in 8.160 secs (750 bytes/sec)
```

- Copiez à partir d'une clé USB ou d'un lecteur interne ou externe :

  copy [**/noconfirm**] **disk***n***:/**[*path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  Exemple :

```
ciscoasa# copy /noconfirm disk1:/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

Copier un fichier dans la configuration de démarrage ou d'exécution

Vous pouvez télécharger un fichier texte pour la configuration de démarrage à partir d'un serveur TFTP, FTP, SMB, HTTP(S) ou SCP, ou à partir de la mémoire flash.

Lorsque vous copiez une configuration dans la configuration en cours d'exécution, vous fusionnez les deux configurations. Une fusion ajoute toutes les nouvelles commandes de la nouvelle configuration à la configuration en cours d'exécution. Si les configurations sont identiques, aucune modification ne se produit. Si des commandes sont en conflit ou si des commandes influent sur le fonctionnement de l'ASA, l'effet de la fusion dépend de la commande. Vous pourriez obtenir des erreurs ou des résultats inattendus.

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

Dans un contexte en mode de contexte multiple, vous pouvez utiliser cette procédure si vous activez le stockage privé (**storage-url private**). Sans stockage privé, pour télécharger à partir d'un serveur TFTP vers la configuration du contexte en cours d'exécution, utilisez la commande **configure net** . SCP n'est pas pris en charge dans un contexte utilisant la pile CiscoSSH

Procédure

Pour copier un fichier dans la configuration de démarrage ou la configuration en cours d'exécution, saisissez l'une des commandes suivantes pour le serveur de téléchargement approprié :

- Copiez à partir d'un serveur TFTP :

  copy [**/noconfirm**] [*interface_name*] **tftp://***server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config
  ```

- Copiez à partir d'un serveur FTP :

  copy [**/noconfirm**] [*interface_name*] **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config
  ```

- Copiez à partir d'un serveur HTTP(S) :

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config
  ```

- Copiez à partir d'un serveur SMB :

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config
  ```

- Copiez à partir d'un serveur SCP :

  copy [**/noconfirm**] [*interface_name*] **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**}

  Exemple :

  ```
  ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config
  ```

L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur SCP.

Exemples

Par exemple, pour copier la configuration à partir d'un serveur TFTP, saisissez la commande suivante :

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

Pour copier la configuration à partir d'un serveur FTP, saisissez la commande suivante :

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

Pour copier la configuration à partir d'un serveur HTTP, saisissez la commande suivante :

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

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

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

Voir les directives suivantes concernant les modèles :

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

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

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

Consultez les paramètres par défaut suivants :

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

Procédure

Étape 1 Définissez l'emplacement de l'image de démarrage de l'ASA :

*URL***du système de démarrage**

Exemple :

```
ciscoasa(config)# boot system disk0:/images/asa921.bin
```

L'URL peut être :

- **disk** *n***:/**[*path*/]*filename*
- **tftp:**//[*utilisateur*[**:***mot de passe*]**@**]*serveur*[**:***port*]/[*chemin*/]*nom de fichier*

  L'option TFTP n'est pas prise en charge sur tous les modèles.

Firepower 1000, 2100 en mode l'appareil, Secure : vous ne pouvez saisir qu'une seule commande **boot system**. Si vous mettez à niveau vers une nouvelle image, vous devez saisir **no boot system** pour supprimer l'image que vous avez définie. Notez que vous ne pouvez pas avoir une commande **boot system** dans votre configuration; par exemple, si vous avez installé l'image de ROMMON, avez un nouveau périphérique ou avez supprimé la commande manuellement. La commande **boot system** exécute une action lorsque vous la saisissez : le système valide et décompresse l'image et la copie dans l'emplacement de démarrage (un emplacement interne sur disk0 géré par FXOS). La nouvelle image sera chargée lorsque vous rechargerez l'ASA. Si vous changez d'avis avant de téléverser, vous pouvez entrer la commande **no boot system** pour supprimer la nouvelle image de l'emplacement de démarrage, de sorte que l'image actuelle continue de s'exécuter. Vous pouvez même supprimer le fichier image original de la mémoire flash de l'ASA après avoir entré cette commande, et l'ASA démarrera correctement à partir de l'emplacement de démarrage; cependant, nous recommandons de conserver toutes les images que vous souhaitez utiliser dans la mémoire flash, car la commande **boot system** ne fonctionne qu'avec les images dans cette dernière. Contrairement à d'autres modèles, cette commande dans la configuration de démarrage n'affecte pas l'image de démarrage et est essentiellement cosmétique. La dernière image de démarrage chargée sera toujours exécutée lors du rechargement. Si vous n'enregistrez pas la configuration après avoir saisi cette commande, l'ancienne commande sera présente dans votre configuration lors du rechargement, même si la nouvelle image a été démarrée. Assurez-vous d'enregistrer la configuration pour qu'elle reste synchronisée. Vous pouvez uniquement téléverser des images avec le nom de fichier d'origine à partir du site de téléchargement de Cisco. Si vous modifiez le nom de fichier, il ne se téléversera pas. Vous pouvez également recréer l'image de Firewall Threat Defense en chargeant l'image Firewall Threat Defense. Dans ce cas, vous êtes invité à téléverser immédiatement.

autres modèles : vous pouvez entrer jusqu'à quatre entrées de commande de **démarrage système** pour définir différentes images de démarrage dans l'ordre; l'ASA démarre la première image qu'il trouve avec succès. Lorsque vous saisissez la commande **boot system** (démarrage système), elle ajoute une entrée au bas de la liste. Pour réorganiser les entrées de démarrage, vous devez supprimer toutes les entrées à l'aide de la commande **clear configure boot system** et les saisir à nouveau dans l'ordre souhaité. Une seule commande **boot system tftp** peut être configurée et elle doit être la première à être configurée.

Remarque
Si l'ASA est bloqué dans un cycle de démarrage constant, vous pouvez le redémarrer en mode ROMMON. Pour plus d'informations sur le mode ROMMON, consultez Afficher les messages de débogage.

Exemple :

```
asa(config)# boot system disk0:/cisco-asa-fp2k.9.13.2.SPA
The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.13.2 will do the following:
   - upgrade to the new platform version 2.7.2
   - upgrade to the CSP ASA version 9.13.2
```

```
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
asa(config)#
```

Étape 2 Définissez l'image ASDM pour démarrer :

asdm image disk*n***:/**[*path*/]*filename*

Exemple :

```
ciscoasa(config)# asdm image disk0:/images/asdm721.bin
```

Si vous ne spécifiez pas l'image au démarrage, même si une seule image est installée, l'ASA insère la commande **asdm image** dans la configuration en cours. Pour éviter des problèmes avec la mise à jour automatique (si elle est configurée) et pour éviter la recherche d'image à chaque démarrage, vous devez préciser l'image ASDM que vous souhaitez démarrer dans la configuration de démarrage.

Étape 3 (Facultatif) Définir la configuration de démarrage de sorte qu'elle utilise un fichier connu au lieu du fichier masqué :

boot config disk*n***:/**[*path*/]*filename*

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

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

Exemple :

```
ciscoasa(config)# boot config disk0:/configs/startup1.cfg
```

Sauvegarde et restauration de configurations ou d'autres fichiers

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

Effectuer une sauvegarde ou une restauration complète du système

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

Avant d'entreprendre la sauvegarde ou la restauration

- Vous devez avoir au moins 300 Mo d'espace disque disponible à l'emplacement de sauvegarde ou de restauration avant de lancer une sauvegarde ou une restauration.
- Si vous apportez des modifications à la configuration pendant ou après une sauvegarde, ces modifications ne seront pas incluses dans la sauvegarde. Si vous modifiez une configuration après avoir effectué la sauvegarde, puis effectuez une restauration, cette modification de configuration sera remplacée. Par conséquent, l'ASA pourrait se comporter différemment.
- Vous ne pouvez lancer qu'une seule sauvegarde ou restauration à la fois.
- Vous pouvez uniquement restaurer une configuration sur la même version ASA que celle lorsque vous avez effectué la sauvegarde d'origine. Vous ne pouvez pas utiliser l'outil de restauration pour migrer une configuration d'une version ASA vers une autre. Si une migration de configuration est requise, l'ASA met automatiquement à niveau la configuration de démarrage résidente lorsqu'il charge le nouveau système d'exploitation de l'ASA.
- Si vous utilisez la mise en grappe, vous pouvez uniquement sauvegarder ou restaurer les certificats de configuration de démarrage, de configuration d'exécution et d'identité. Vous devez créer et restaurer une sauvegarde séparément pour chaque unité.
- Si vous utilisez le basculement, vous devez créer et restaurer une sauvegarde séparément pour les unités actives et de secours.
- Si vous définissez une phrase secrète principale pour l'ASA, vous avez besoin de cette phrase secrète principale pour restaurer la configuration de sauvegarde que vous créez avec cette procédure. Si vous ne connaissez pas la phrase secrète principale pour l'ASA, consultez Configurer la phrase secrète principale pour savoir comment la réinitialiser avant de poursuivre la sauvegarde.
- Si vous importez des données PKCS12 (avec la commande **crypto ca trustpoint**) et que le point de confiance utilise des clés RSA, la paire de clés importée se voit attribuer le même nom que le point de confiance. En raison de cette limite, si vous spécifiez un nom différent pour le point de confiance et sa paire de clés après avoir restauré une configuration ASDM, la configuration de démarrage sera la même que la configuration d'origine, mais la configuration d'exécution comprendra un nom de paire de clés différent. Cela signifie que si vous utilisez des noms différents pour la paire de clés et le point de confiance, vous ne pouvez pas restaurer la configuration d'origine. Pour contourner ce problème, assurez-vous d'utiliser le même nom pour le point de confiance et sa paire de clés.
- Vous ne pouvez pas sauvegarder à l'aide de l'interface de ligne de commande et restaurer à l'aide d'ASDM, ou inversement.
- Chaque fichier de sauvegarde comprend le contenu suivant :
  - Configuration d'exécution
  - Configuration du démarrage
  - Toutes les images de sécurité

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

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

    Images et profils (SVC) d'Secure Client (services client sécurisés)

    Personnalisations et transformations (SVC) d'Secure Client (services client sécurisés)

- Certificats d'identité (inclut les paires de clés RSA liées aux certificats d'identité; exclut les clés autonomes)
- Clés prépartagées VPN
- Configurations SSL VPN
- Cadre personnalisé du profil d'application (APCF)
- Signets
- Personnalisations
- Politique d'accès dynamique (DAP)
- Modules d'extension
- Scripts de préremplissage pour les profils de connexion
- Configuration automatique du serveur mandataire
- Table de traduction
- Web content
- Information de version

Sauvegarder le système

Cette procédure décrit comment effectuer une sauvegarde complète du système.

Procédure

Étape 1 Sauvegardez le système :

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

Exemple :

```
ciscoasa# backup location disk0:/sample-backup]
Backup location [disk0:/sample-backup]?
```

Si vous ne spécifiez pas de **nom** *d'interface*, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

En mode de contexte multiple à partir de l'espace d'exécution du système, saisissez le mot clé **context** pour sauvegarder le contexte spécifié. Chaque contexte doit être sauvegardé individuellement; c'est-à-dire que vous devez saisir à nouveau la commande **backup** pour chaque fichier.

Lors de la sauvegarde des certificats VPN et des clés prépartagées, une clé secrète identifiée par le mot clé **passphrase** est requise pour encoder les certificats. Vous devez fournir une phrase secrète à utiliser pour l'encodage et le décodage des certificats au format PKCS12. La sauvegarde comprend uniquement les paires de clés RSA liées aux certificats et exclut tout certificat autonome.

L'**emplacement** de sauvegarde peut être un disque local ou une URL distante. Si vous ne fournissez pas d'emplacement, les noms par défaut suivants sont utilisés :

- Mode unique—disk0 :*hostname*.backup.*timestamp*.tar.gz
- Mode multiple—disk0 :*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

Étape 2 Suivez les instructions :

Exemple :

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco.
You will be required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file
is used to restore to a device with a different master passphrase,
you will need to provide the current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

Restaurer la sauvegarde

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

Procédure

Étape 1 Restaurez le système à partir du fichier de sauvegarde.

restore [**/noconfirm**] [**context** *ctx-name*] [**passphrase** *value*] [**location** *path*]

Exemple :

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
```

```
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
```

Lorsque vous utilisez le mot clé **context** pour restaurer plusieurs contextes, chaque fichier de contexte sauvegardé doit être restauré individuellement; c'est-à-dire que vous devez saisir à nouveau la commande **restore** pour chaque fichier.

Étape 2 Suivez les instructions :

Exemple :

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version,
some configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption.
Master passphrase is required to restore running configuration,
startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to
this device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside,
the IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside,
the IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations.
Do not overwrite configuration file if you want to preserve the old http-
and https-proxy configurations.

Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates.
The default is cisco. If the passphrase is not correct, certificates will not be restored.
```

```
No passphrase was provided for identity certificates.
Using the default value: cisco. If the passphrase is not correct,
certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

Configurer la sauvegarde et la restauration automatiques (ISA 3000)

Sur l'ISA 3000, vous pouvez configurer des sauvegardes automatiques vers un emplacement particulier chaque fois que vous enregistrez votre configuration à l'aide de **write memory**.

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

Configurer la sauvegarde automatique (ISA 3000)

Sur l'ISA 3000, vous pouvez configurer des sauvegardes automatiques vers un emplacement particulier chaque fois que vous enregistrez votre configuration à l'aide de **write memory**.

Avant de commencer

Cette fonctionnalité est uniquement disponible sur l'ISA 3000.

Procédure

Étape 1 Définissez les paramètres du paquet de sauvegarde :

backup-package backup [**interface** *name*] **location** {**disk***n***:** | *url*} [**passphrase** *string*]

- **interface** *name* : spécifie l'interface permettant d'atteindre l'URL de sauvegarde, si vous spécifiez un stockage hors périphérique. Si vous ne spécifiez pas de nom d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.
- **location** {**disk***n***:** | *url*} : spécifie le support de stockage à utiliser pour la sauvegarde des données. Vous pouvez définir une URL ou un stockage local : disk0 est le lecteur flash interne, disk1 est une clé de mémoire USB facultative sur USB 1, disk2 est une clé de mémoire USB facultative sur USB 2. Et disk3 est la carte mémoire SD. Notez que les paramètres par défaut pour la restauration automatique utilisent disk3.
- **passphrase** *string* : définit la phrase secrète pour sécuriser les données sauvegardées. Notez que les paramètres par défaut pour la restauration automatique utilisent « cisco » comme phrase secrète.

Ces paramètres sont également utilisés par défaut avec la commande manuelle **backup**. Consultez Sauvegarder le système, à la page 25. Notez que si vous utilisez la commande manuelle **backup** lorsque la sauvegarde ou

la restauration automatiques sont activées, le système enregistre un fichier de sauvegarde avec le nom spécifié, ainsi que le nom « auto-backup-asa.tgz » utilisé par la sauvegarde et la restauration automatiques.

Exemple :

```
ciscoasa(config)# backup-package backup location disk3: passphrase cisco
```

Étape 2 Activez le mode automatique pour la sauvegarde et la restauration :

backup-package backup auto

Lorsque vous enregistrez la configuration à l'aide de **write memory**, la configuration est automatiquement enregistrée à l'emplacement de sauvegarde ainsi que dans la configuration de démarrage. Le fichier de sauvegarde est intitulé « auto-backup-asa.tgz ». Pour désactiver les sauvegardes automatiques, utilisez la forme **no** de la commande.

Exemple :

```
ciscoasa(config)# backup-package backup auto
```

Configurer la restauration automatique (ISA 3000)

Le mode de restauration automatique restaure la configuration système sur un périphérique sans intervention de l'utilisateur. Par exemple, vous insérez une carte de mémoire SD contenant une configuration de sauvegarde enregistrée dans un nouveau périphérique, puis mettez celui-ci sous tension. Lorsque le périphérique se manifeste, il vérifie la carte SD pour décider si la configuration système doit être restaurée. (La restauration n'est lancée que si le fichier de sauvegarde comporte l'« empreinte digitale » d'un autre périphérique. L'empreinte du fichier de sauvegarde est mise à jour pour correspondre au périphérique actuel lors d'une opération de sauvegarde ou de restauration. Donc, si le périphérique a déjà effectué une restauration ou s'il a créé sa propre sauvegarde, la restauration automatique est ignorée.) Si l'empreinte indique qu'une restauration est requise, le périphérique remplace la configuration système (startup-config, running-config, configuration du SSL VPN, etc.; consultez Sauvegarder le système, à la page 25 pour plus de détails sur le contenu de la sauvegarde). Lorsque le périphérique a terminé son démarrage, il exécute la configuration enregistrée.

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

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

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

  La valeur par défaut est **auto**.

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

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

- **RESTORE_PASSPHRASE** = *key*

  La valeur par défaut est **cisco**.

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

Avant de commencer

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

Procédure

Étape 1 Définissez les paramètres du paquet de restauration.

backup-package restore location {**disk***n***:** | *url*} [**passphrase** *string*]

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

Ces paramètres sont également utilisés par défaut avec la commande manuelle **restore**. Consultez Sauvegarder le système, à la page 25.

Exemple :

```
ciscoasa(config)# backup-package restore location disk1: passphrase $upe3rnatural
```

Étape 2 Activez ou désactivez le mode automatique pour la restauration.

[**no**]**backup-package restore auto**

Le nom du fichier restauré est « auto-backup-asa.tgz ».

Exemple :

```
ciscoasa(config)# no backup-package restore auto
```

Sauvegarder la configuration en mode unique ou la configuration système en mode multiple

En mode de contexte unique ou à partir de la configuration système en mode multiple, vous pouvez copier la configuration de démarrage ou la configuration en cours d'exécution sur un serveur externe ou dans la mémoire flash locale.

Avant de commencer

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

Procédure

Sauvegardez la configuration en utilisant l'un des types de serveur suivants :

- Copiez sur un serveur TFTP :

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **tftp:**//*server*[/*path*]/*dst_filename*

  Exemple :

  ```
  ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg
  ```

- Copiez sur un serveur FTP :

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **ftp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  Exemple :

  ```
  ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg
  ```

- Copiez sur un serveur SMB :

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **smb:**//[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  Exemple :

  ```
  ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg
  ```

- Copiez sur un serveur SCP :

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **scp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*[**;int=***interface_name*]

  Exemple :

  ```
  ciscoasa# copy startup-config
  ```

```
scp://pilot:moya@10.86.94.170/new-startup.cfg
```

L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur SCP.

- Copiez dans la mémoire flash locale :

  copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  Exemple :

```
ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg
```

  Assurez-vous que le répertoire de destination existe. S'il n'existe pas, créez d'abord le répertoire à l'aide de la commande **mkdir**.

Sauvegarder une configuration de contexte ou un autre fichier dans la mémoire flash

Copiez les configurations de contexte ou les autres fichiers qui se trouvent sur la mémoire flash locale en saisissant l'une des commandes suivantes dans l'espace d'exécution du système.

Avant de commencer

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

Procédure

Sauvegardez une configuration de contexte en utilisant l'un des types de serveur suivants :

- Copiez depuis la mémoire flash vers un serveur TFTP :

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **tftp://***server*[*/path*]*/dst_filename*

  Exemple :

```
ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin
```

- Copiez depuis la mémoire flash vers un serveur FTP :

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  Exemple :

```
ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin
```

- Copiez depuis la mémoire flash vers un serveur SMB :

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  Exemple :

  ```
  ciscoasa# copy /noconfirm copy disk0:/asdm.bin
  smb://chiana:dargo@10.1.1.67/asdm.bin
  ```

- Copiez depuis la mémoire flash vers un serveur SCP :

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  Exemple :

  ```
  ciscoasa# copy disk0:/context1.cfg
  scp://pilot:moya@10.86.94.170/context1.cfg
  ```

  L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur SCP.

- Copiez depuis la mémoire flash vers la mémoire flash locale :

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  Exemple :

  ```
  ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg
  ```

  Assurez-vous que le répertoire de destination existe. S'il n'existe pas, créez d'abord le répertoire à l'aide de la commande **mkdir**.

Sauvegarder une configuration de contexte dans un contexte

En mode de contexte multiple, à partir d'un contexte, vous pouvez effectuer les sauvegardes suivantes.

Procédure

Étape 1 Copiez la configuration en cours d'exécution à l'emplacement de la configuration de démarrage (si, sur un serveur distant, elle est connectée au contexte d'administration). L'emplacement de la configuration de démarrage est spécifié par la commande **config-url**.

copy running-config startup-config

Exemple :

```
ciscoasa/contexta# copy running-config startup-config
```

Étape 2 Copiez la configuration en cours d'exécution sur un serveur FTP ou TFTP connecté au réseau *contextuel*.

copy running-config {**ftp** | **tftp**}**:**//*url*/*dest_filename*

Consultez l'aide de la commande **copy** pour connaître les options d'URL exactes.

Si vous activez le stockage privé (**storage-url private**), d'autres options de serveur sont disponibles. Cependant, SCP n'est pas pris en charge dans un contexte utilisant la pile CiscoSSH.

Exemple :

```
ciscoasa/contexta# copy running-config tftp:/10.89.6.8/configs/1010-1.cfg
```

Copier la configuration à partir de l'affichage du terminal

Procédure

Étape 1 Imprimez la configuration sur le terminal :

more system:running-config

Étape 2 Copiez le résultat de cette commande, puis collez la configuration dans un fichier texte.

Sauvegarder les fichiers supplémentaires à l'aide des commandes d'exportation et d'importation

Les fichiers supplémentaires essentiels à votre configuration peuvent inclure les éléments suivants :

- Les fichiers que vous importez à l'aide de la commande **import webvpn**. Actuellement, ces fichiers comprennent les personnalisations, les listes d'URL, le contenu Web, les modules d'extension et les traductions de langue.
- Politiques DAP (dap.xml).
- Configurations CSD (data.xml).
- Clés et certificats numériques.
- Base de données des utilisateurs CA locale et fichiers d'état des certificats.

L'interface de ligne de commande vous permet de sauvegarder et de restaurer des éléments individuels de votre configuration à l'aide des commandes **export** et **import**.

Pour sauvegarder ces fichiers, par exemple, les fichiers que vous avez importés avec la commande **import webvpn** ou les certificats, procédez comme suit.

Procédure

Étape 1 Exécutez la ou les commandes **show** applicables comme suit :

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

Étape 2 Exécutez la commande **export** pour le fichier que vous souhaitez sauvegarder (dans cet exemple, le fichier rdp) :

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

Utiliser un script pour sauvegarder et restaurer des fichiers

Vous pouvez utiliser un script pour sauvegarder et restaurer les fichiers de configuration de votre ASA, y compris toutes les extensions que vous importez via l'interface de ligne de commande **import webvpn**, les fichiers XML de configuration CSD et le fichier XML de configuration DAP. Pour des raisons de sécurité, nous vous déconseillons d'effectuer des sauvegardes automatisées des clés et des certificats numériques ou de la clé CA locale.

Cette section fournit des instructions à cet effet et comprend un exemple de script que vous pouvez utiliser tel quel ou modifier en fonction de votre environnement. L'exemple de script est propre à un système Linux. Pour l'utiliser sur un système Microsoft Windows, vous devez le modifier en utilisant la logique de l'exemple.

Remarque Vous pouvez également utiliser les commandes **backup** et **restore**. Consultez Effectuer une sauvegarde ou une restauration complète du système, à la page 23 pour de plus amples renseignements.

Avant d'utiliser des scripts de sauvegarde et de restauration

Si vous souhaitez utiliser un script pour sauvegarder et restaurer une configuration ASA, effectuez d'abord les tâches suivantes :

- Installez Perl avec un module Expect.
- Installez un client SSH qui peut atteindre l'ASA.
- Installez un serveur TFTP pour envoyer des fichiers de l'ASA vers le site de sauvegarde.

Une autre option consiste à utiliser un outil disponible dans le commerce. Vous pouvez placer la logique de ce script dans un tel outil.

Exécuter le script

Pour exécuter un script de sauvegarde et de restauration, procédez comme suit.

Procédure

Étape 1 Téléchargez ou copiez et collez le fichier de script à n'importe quel emplacement de votre système.

Étape 2 Dans la ligne de commande, saisissez **Perl***scriptname*, où *scriptname* est le nom du fichier de script.

Étape 3 Appuyez sur **Entrée**.

Étape 4 Le système vous invite à saisir des valeurs pour chaque option. Vous pouvez également saisir des valeurs pour les options lorsque vous saisissez la commande **Perl***scriptname* avant d'appuyer sur **Enter** (Entrée). Dans tous les cas, le script exige que vous saisissiez une valeur pour chaque option.

Étape 5 Le script commence à s'exécuter et affiche les commandes qu'il émet, ce qui vous fournit un enregistrement des interfaces de ligne de commande. Vous pouvez utiliser ces interfaces de ligne de commande pour une restauration ultérieure, ce qui est particulièrement utile si vous ne souhaitez restaurer qu'un ou deux fichiers.

Exemple de script

```
#!/usr/bin/perl
#Description: The objective of this script is to show how to back up
configurations/extensions.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#       -r: Restore with an argument that specifies the file name. This file is produced
during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F`;
chop($date);
my $exp = new Expect();
```

```
getopts("h:u:p:w:e:s:r:",\%options);
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("$enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
```

```
  print "$cli\n";
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}


sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub url_list {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn url-list\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
     $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
```

```
      $obj->send("$cli\n");
      $obj->expect(15, "$prompt#" );
   }
}

sub dap {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir dap.xml\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub csd {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir sdesktop\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub webcontent {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn webcontent\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /No custom/;
     next unless (/^.+\s+.+$/);
     ($url, $type) = split(/\s+/,$_);
     $turl = $url;
     $turl =~ s/\/\+//;
     $turl =~ s/\+\//-/;
     $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
```

```
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}

sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
      $storage = "tftp://$tstr";
  }
  else {
      print "Enter TFTP host name or IP address:";
      chop($tstr=<>);
      $storage = "tftp://$tstr";
  }
  if (defined($options{h})) {
      $asa = $options{h};
  }
  else {
      print "Enter ASA host name or IP address:";
      chop($asa=<>);
  }

  if (defined ($options{u})) {
      $user= $options{u};
  }
  else {
      print "Enter user name:";
      chop($user=<>);
  }
```

```
  if (defined ($options{w})) {
      $password= $options{w};
  }
  else {
      print "Enter password:";
      chop($password=<>);
  }
  if (defined ($options{p})) {
      $prompt= $options{p};
  }
  else {
      print "Enter ASA prompt:";
      chop($prompt=<>);
  }
  if (defined ($options{e})) {
      $enable = $options{e};
  }
  else {
      print "Enter enable password:";
      chop($enable=<>);
  }

  if (defined ($options{r})) {
     $restore = 1;
     $restore_file = $options{r};
  }
}
```

Échange à chaud d'un SSD sur Cisco Secure Firewall

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

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

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

Procédure

Étape 1 Retirez l'un des disques SSD.

a) Retirez le SSD du RAID.

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

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

Exemple :

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

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

show raid

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

Exemple :

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

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

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

ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
```

```
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

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

c) Retirez physiquement le disque SSD du châssis.

Étape 2 Ajouter un disque SSD.

a) Ajoutez physiquement le SSD dans le logement vide.

b) Ajoutez le SSD au RAID.

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

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

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

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

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

Historique des logiciels et des configurations

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Client et serveur Secure Copy	9.1(5)/9.2(1)	L'ASA prend désormais en charge le client et le serveur Secure Copy (SCP) pour transférer des fichiers vers et depuis un serveur SCP. Nous avons introduit les commandes suivantes : **ssh pubkey-chain**, **server (ssh pubkey-chain)**, **key-string**, **key-hash**, **ssh stricthostkeycheck**. Nous avons modifié la commande suivante : **copy scp**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Chiffrement SSH et d'intégrité configurables	9.1(7)9.4(3)9.5(3)9.6(1)	Les utilisateurs peuvent sélectionner des modes de chiffrement lors de la gestion du chiffrement SSH et peuvent configurer le HMAC et le chiffrement pour divers algorithmes d'échange de clés. Vous souhaiterez peut-être modifier les chiffres pour qu'ils soient plus ou moins stricts, selon votre application. Notez que la performance de la copie sécurisée dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier les chiffres proposés, utilisez **ssh cipher encryption custom aes128-cbc**, par exemple. Nous avons introduit les commandes suivantes : **ssh cipher encryption**, **ssh cipher integrity**
Vérification du certificat du serveur de mise à jour automatique activée par défaut	9.2(1)	La vérification du certificat du serveur de mise à jour automatique est maintenant activée par défaut; pour les nouvelles configurations, vous devez explicitement désactiver la vérification de certificat. Si vous effectuez une mise à niveau à partir d'une version antérieure et que vous n'avez pas activé la vérification de certificat, la vérification de certificat n'est pas activée, et l'avertissement suivant s'affiche : `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` La configuration sera migrée vers la configuration explicite sans vérification. **auto-update server no-verification** Nous avons modifié la commande suivante : **auto-update server** {**verify-certificate** | **no-verification**}.
Sauvegarde et restauration du système à l'aide de l'interface de ligne de commande	9.3(2)	Vous pouvez maintenant sauvegarder et restaurer des configurations système complètes, y compris les images et les certificats, à l'aide de l'interface de ligne de commande. Nous avons introduit les commandes suivantes : **backup** et **restore**.
Récupération et chargement d'une nouvelle image ASA 5506W-X	9.4(1)	Nous prenons désormais en charge la récupération et le chargement d'une nouvelle image ASA 5506W-X. Nous avons introduit la commande suivante : **hw-module module wlan recover image**.

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

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.