Guide de mise à niveau de Cisco Secure Firewall ASA

Dernière modification : 2025-05-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

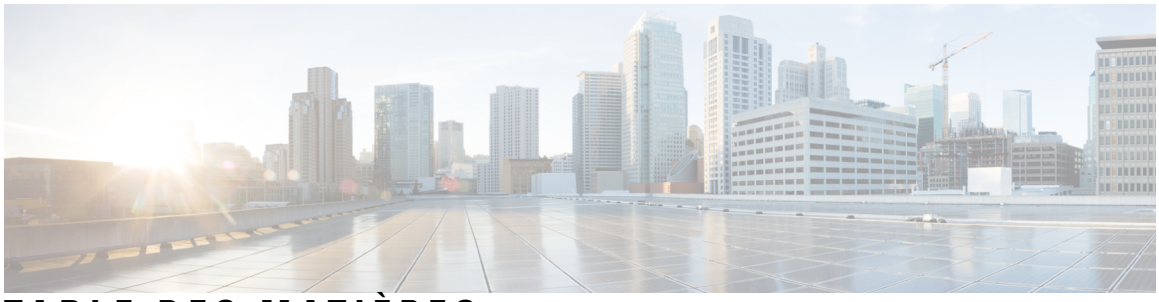


TABLE DES MATIÈRES

CHAPITRE 1 **Planification de votre mise à niveau** 1

Directives importantes avant d'effectuer une mise à niveau 1

Lignes directrices pour la mise à niveau de l'ASA 1

Directives et migrations propres à la version 1

Directives de mise en grappe 19

Directives en matière de basculement 22

Directives supplémentaires 23

Directives de mise à niveau de FXOS 24

Liste de contrôle pour la mise à niveau d'ASA 24

Compatibilité 25

Compatibilité ASA et ASDM par modèle 25

ASA 9.22 25

ASA 9.20 et 9.19 26

ASA 9.18 à 9.17 27

ASA 9.16 à 9.15 28

ASA 9.14 à 9.13 30

ASA 9.12 à 9.5 31

Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces 33

Compatibilité avec Radware DefensePro 40

Chemin de mise à niveau 45

Chemin de mise à niveau : Appareils ASA 45

Chemin de mise à niveau : ASA sur Firepower 2100 en mode plateforme 52

Chemin de mise à niveau : périphériques logiques ASA pour le Firepower 4100/9300 55

Télécharger le logiciel à partir de Cisco.com 61

Télécharger le logiciel ASA 61

Télécharger FXOS pour le Firepower 4100/9300 73

Sauvegarder vos configurations 73

CHAPITRE 2 **Mettre à niveau l'ASA 75**

Mettre à niveau l'appareil ASA 75

Mettre à niveau une unité autonome 75

Mettre à niveau une unité autonome à l'aide de l'interface de ligne de commande 75

Mettre à niveau une unité autonome à partir de votre ordinateur local à l'aide d'ASDM 77

Mettre à niveau une unité autonome à l'aide de l'assistant ASDM Cisco.com 79

Mettre à niveau une paire de basculements actif/de secours 80

Mettre à niveau une paire de basculements actif/de secours à l'aide de l'interface de ligne de commande 80

Mettre à niveau une paire de basculements actif/de secours à l'aide d'ASDM 83

Mettre à niveau une paire de basculements actif/actif 84

Mettre à niveau une paire de basculements actif/actif à l'aide de l'interface de ligne de commande 84

Mettre à niveau une paire de basculements actif/actif à l'aide d'ASDM 87

Mettre à niveau une grappe ASA (Secure Firewall 3100/4200) 89

Mettre à niveau une grappe ASA à l'aide de l'interface de ligne de comande (Secure Firewall 3100/4200) 89

Mettre à niveau une grappe ASA à l'aide d'ASDM (Secure Firewall 3100/4200) 92

Mettre à niveau le Firepower 4100/9300 94

Mettre à niveau FXOS et un périphérique autonome ASA ou une grappe intra-châssis 95

Mettre à niveau FXOS et un périphérique autonome ASA ou une grappe intra-châssis à l'aide de Cisco Secure Firewall Chassis Manager 95

Mettre à niveau FXOS et un périphérique autonome ASA ou une grappe intra-châssis à l'aide de l'interface de ligne de commande de FXOS 96

Mettre à niveau FXOS et une paire de basculements ASA actif/de secours 99

Mettre à niveau FXOS et une paire de basculements ASA actif/de secours à l'aide de Cisco Secure Firewall Chassis Manager 99

Mettre à niveau FXOS et une paire de basculements ASA actif/de secours à l'aide de l'interface de ligne de commande de FXOS 102

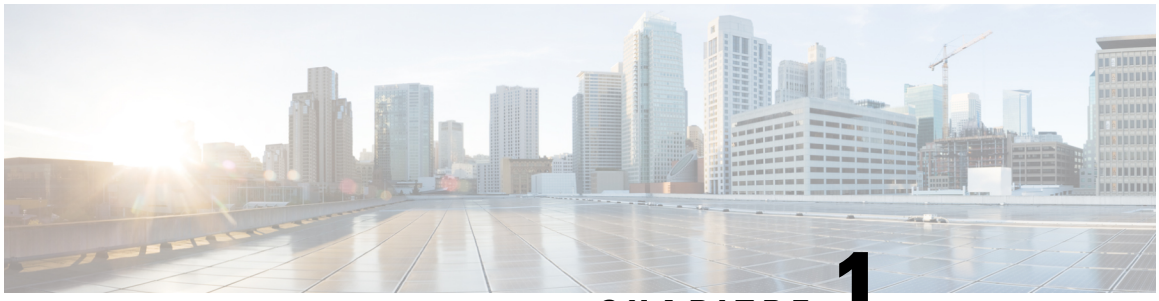
Mettre à niveau FXOS et une paire de basculements ASA actif/actif 110

Mettre à niveau FXOS et une paire de basculements ASA actif/actif à l'aide de Cisco Secure Firewall Chassis Manager 110

Mettre à niveau FXOS et une paire de basculements ASA actif/actif à l'aide de l'interface de ligne de commande de FXOS 113
Mettre à niveau FXOS et une grappe inter-châssis ASA 122
Mettre à niveau FXOS et une grappe inter-châssis ASA à l'aide de Cisco Secure Firewall Chassis Manager 122
Mettre à niveau FXOS et une grappe inter-châssis ASA à l'aide de l'interface de ligne de commande de FXOS 123
Surveiller l'avancement de la mise à niveau 127
Vérifier l'installation 128
Mettre à niveau l'ASA Virtual, l'ISA 3000 ou l'ASA 5500-X 129
Mettre à niveau une unité autonome 129
Mettre à niveau une unité autonome à l'aide de l'interface de ligne de commande 129
Mettre à niveau une unité autonome à partir de votre ordinateur local à l'aide d'ASDM 131
Mettre à niveau une unité autonome à l'aide de l'assistant ASDM Cisco.com 133
Mettre à niveau une paire de basculements actif/de secours 135
Mettre à niveau une paire de basculements actif/de secours à l'aide de l'interface de ligne de commande 135
Mettre à niveau une paire de basculements actif/de secours à l'aide d'ASDM 138
Mettre à niveau une paire de basculements actif/actif 139
Mettre à niveau une paire de basculements actif/actif à l'aide de l'interface de ligne de commande 139
Mettre à niveau une paire de basculements actif/actif à l'aide d'ASDM 142
Mettre à niveau une grappe ASA 144
Mettre à niveau une grappe ASA à l'aide de l'interface de ligne de commande 144
Mettre à niveau une grappe ASA à l'aide d'ASDM 150
Mettre à niveau le Firepower 2100 en mode plateforme 153
Mettre à niveau une unité autonome 153
Mettre à niveau une unité autonome à l'aide de Firepower Chassis Manager 153
Mettre à niveau une unité autonome à l'aide de l'interface de ligne de commande de FXOS 154
Mettre à niveau une paire de basculements actif/de secours 157
Mettre à niveau une paire de basculements actif/de secours à l'aide de Firepower Chassis Manager 157
Mettre à niveau une paire de basculements actif/de secours à l'aide de l'interface de ligne de commande de FXOS 158
Mettre à niveau une paire de basculements actif/actif 164

Mettre à niveau une paire de basculements actif/actif à l'aide de Firepower Chassis Manager 164
Mettre à niveau une paire de basculements actif/actif à l'aide de l'interface de ligne de commande de FXOS 166

CHAPITRE 3 **Rétrograder l'ASA 173**
Directives et limites en matière de rétrogradation 173
Configuration incompatible supprimée après la rétrogradation 175
Rétrograder l'appareil ASA 176
Rétrograder le Firepower 2100 en mode plateforme 177
Rétrograder le Firepower 4100/9300 177
Rétrograder l'ISA 3000 ou l'ASA 5500-X 178



CHAPITRE 1

Planification de votre mise à niveau

Avant de mettre à niveau le Secure Firewall ASA, vous devez effectuer la préparation suivante :

- Vérifiez le chemin de mise à niveau de la version actuelle vers la version cible. Assurez-vous de planifier les versions intermédiaires requises pour chaque système d'exploitation.
- Vérifiez les directives et les limites qui concernent vos versions intermédiaires et cibles, ou qui influent sur la mise à niveau du basculement et de la mise en grappe sans temps d'arrêt.
- Téléchargez tous les paquets de logiciels requis à partir de Cisco.com.
- Sauvegardez vos configurations, surtout en cas de migration de configuration.

Les rubriques suivantes expliquent comment mettre à niveau votre instance d'ASA.

- Directives importantes avant d'effectuer une mise à niveau, à la page 1
- Liste de contrôle pour la mise à niveau d'ASA, à la page 24
- Compatibilité, à la page 25
- Chemin de mise à niveau, à la page 45
- Télécharger le logiciel à partir de Cisco.com, à la page 61
- Sauvegarder vos configurations, à la page 73

Directives importantes avant d'effectuer une mise à niveau

Vérifiez les directives et les limites de mise à niveau, ainsi que les migrations de configuration pour chaque système d'exploitation.

Lignes directrices pour la mise à niveau de l'ASA

Avant de procéder à une mise à niveau, vérifiez les migrations et toute autre directive.

Directives et migrations propres à la version

Selon votre version actuelle, vous pourriez rencontrer une ou plusieurs migrations de configuration et devrez peut-être tenir compte des directives de configuration pour toutes les versions entre la version de début et la version de fin lorsque vous effectuez une mise à niveau.

Directives sur 9.22

- **Transport par défaut de la licence Smart modifié dans la version 9.22** : dans la version 9.22, le transport par défaut de la licence Smart est passé de Smart Call Home à Smart Transport. Vous pouvez configurer l'ASA pour utiliser Smart Call Home au besoin en utilisant la commande **transport type callhome**. Lorsque vous effectuez une mise à niveau vers la version 9.22, le transport passe automatiquement à Smart Transport. Si vous effectuez une rétrogradation, le transport est rétabli à Smart Call Home, et si vous souhaitez utiliser Smart Transport, vous devez préciser **transport type smart**.

Directives sur 9.20

- **Les commandes de redistribution OSPFv3 qui précisent une carte de routage correspondant à une liste de préfixes seront supprimées dans la version 9.20(2)** : lorsque vous passez à la version 9.20(2), les commandes de **redistribution** OSPFv3 où la **carte de routage** indiquée utilise une **liste de préfixes d'adresse IP correspondante** seront supprimées de la configuration. Bien que les listes de préfixes n'aient jamais été prises en charge, l'analyseur a toujours accepté la commande. Avant la mise à niveau, vous devez reconfigurer OSPFv3 de manière à utiliser les cartes de routage qui précisent une liste de contrôle d'accès dans la commande **match ip address**.

Rappel La redistribution des cartes de routage avec la liste de préfixes IPv4 sur OSPFv2 est prise en charge.

Directives sur 9.19

- **ASDM 7.19(1) requiert la version 8u261 d'Oracle Java ou une version ultérieure.**– Avant de passer à ASDM 7.19, assurez-vous de mettre à jour Oracle Java (si utilisé) à la version 8u261 ou plus récente. Cette version prend en charge TLSv1.3, qui est nécessaire pour mettre à jour le lanceur ASDM. OpenJRE n'est pas concerné.

Directives sur 9.18

- **Prise en charge des images signées ASDM dans la version 9.18(2)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)
- **Problème de mise à niveau de la version 9.18(1) si vous avez activé HTTPS/ASDM (avec authentification HTTPS) et SSL sur la même interface avec le même port** : si vous activez à la fois l'accès SSL (**webvpn** > **activer** *l'interface*) et l'accès HTTPS/ASDM (**http**) sur la même interface, vous pouvez accéder à AnyConnect à partir de l'adresse **https://***ip_address* et à ASDM à partir de l'adresse **https://***ip_address***/admin**, tous deux sur le port 443. Cependant, si vous activez également l'authentification HTTPS (**aaa authentication http console**), vous devez définir un port différent pour l'accès ASDM à partir de la version 9.18(1). Assurez-vous de modifier le port avant de procéder à la mise à niveau à l'aide de la commande **http**. (CSCvz92016)
- **Assistant de mise à niveau ASDM** : en raison de la migration de l'API ASD, vous devez utiliser ASDM 7.18 ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.18 ou une version

ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM vers la version 7.18 ou une version ultérieure pour n'importe quelle version d'ASA.

Directives sur 9.17

- **Prise en charge des images signées ASDM dans la version 9.17(1.13)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)
- **Aucune prise en charge du VPN SSL sans client dans les versions 9.17(1) et les versions ultérieures** : le VPN SSL sans client n'est plus pris en charge.
  - **webvpn** : les sous-commandes suivantes sont supprimées :
    - **apcf**
    - **java-trustpoint**
    - **onscreen-keyboard**
    - **port-forward**
    - **portal-access-rule**
    - **rewrite**
    - **smart-tunnel**
  - **group-policy webvpn** : les sous-commandes suivantes sont supprimées :
    - **port-forward**
    - **smart-tunnel**
    - **ssl-clientless**
- **Assistant de mise à niveau ASDM** : en raison d'un changement interne, à partir de mars 2022, l'assistant de mise à niveau ne fonctionnera plus avec les versions antérieures à ASDM 7.17(1.152). Vous devez procéder à une mise à niveau manuelle vers la version 7.17(1.152) ou une version ultérieure pour utiliser l'assistant.

Directives sur 9.16

- **Prise en charge des images signées ASDM dans la version 9.16(3.19)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)

- **Les utilisateurs SNMPv3 utilisant le hachage MD5 et le chiffrement DES ne sont plus pris en charge, et les utilisateurs seront supprimés lors de la mise à niveau vers la version 9.16(1) :** assurez-vous de modifier toute configuration utilisateur pour utiliser des algorithmes de sécurité plus élevés à l'aide de la commande **snmp-server user** avant d'effectuer la mise à niveau.
- **Action de la clé d'hôte SSH requise dans la version 9.16(1)** : en plus de RSA, nous avons ajouté la prise en charge des clés d'hôte EDDSA et ECDSA pour SSH. L'ASA essaie d'utiliser les clés dans l'ordre suivant, si elles existent : EDDSA, ECDSAA, puis RSA. Lorsque vous effectuez une mise à niveau vers la version 9.16(1), l'ASA utilisera la clé RSA existante. Cependant, nous vous recommandons de générer des clés de sécurité élevée dès que possible à l'aide de la commande **crypto key generate** {**eddsa** | **ecdsa**]. De plus, si vous configurez explicitement l'ASA pour utiliser la clé RSA avec la commande **ssh key-exchange hostkey rsa**, vous devez générer une clé de 2 048 bits ou plus. Pour des raisons de compatibilité avec les mises à niveau, l'ASA utilisera des clés hôtes RSA de plus petite taille uniquement lorsque le paramètre par défaut de la clé hôte est utilisé. La prise en charge de RSA sera supprimée dans une version ultérieure.
- **Dans la version 9.16 et les versions ultérieures, les certificats avec des clés RSA ne sont pas compatibles avec les chiffrements ECDSA** : lorsque vous utilisez le groupe de chiffrement ECDHE_ECDSA, configurez le point de confiance avec un certificat qui contient une clé compatible avec ECDSA.
- **ssh version commande supprimée dans la version 9.16(1)** : cette commande a été supprimée. Seule la version 2 du protocole SSH est prise en charge.
- **Lors de la mise à niveau vers la version 9.16 ou une version ultérieure, il se peut que vous voyiez un numéro de série de certificat différent**. Dans la version 9.16, l'ASA a commencé à utiliser OpenSSL, ce qui entraîne un calcul différent des valeurs négatives dans les certificats. Il se peut donc que vous voyiez un numéro de série différent après la mise à niveau. Cette modification n'a pas d'incidence sur le fonctionnement. (CSCvv30338)
- **Fonctionnalité SAMLv1 supprimée dans la version 9.16(1) :** la prise en charge de SAMLv1 a été supprimée.
- **Aucune prise en charge des groupes DH 2, 5 et 24 dans la version 9.16(1)** : la prise en charge a été supprimée pour les groupes DH 2, 5 et 24 dans la configuration des groupes DH SSL. La commande **ssl dh-group** a été mise à jour pour supprimer les options de commande **group2**, **group5** et **group24**.

Directives sur 9.15

- **L'ASA 9.15(1) et les versions ultérieures ne prennent pas en charge les ASA 5525-X, ASA 5545-X et ASA 5555-X.**L'ASA 9.14(x) est la dernière version prise en charge. Pour le module ASA FirePOWER, la dernière version prise en charge est la version 6.6.
- **Cisco annonce l'abandon de la fonctionnalité pour le VPN SSL sans fil avec la version 9.17(1) de l'ASA.**La prise en charge limitée restera valable pour les versions antérieures à la version 9.17(1).
- **Pour le Firepower 1010, la présence d'identifiants de VLAN non valides peuvent causer des problèmes.** Avant d'effectuer une mise à niveau vers la version 9.15(1), assurez-vous de ne pas utiliser de VLAN pour les ports de commutation de la plage de 3968 à 4047. Ces identifiants sont pour un usage interne uniquement, et la version 9.15(1) comprend une vérification pour vous assurer de ne pas utiliser ces identifiants. Par exemple, si ces identifiants sont utilisés après la mise à niveau d'une paire de basculements, la paire de basculements passera à l'état suspendu. Consultez le bogue CSCvw33057 pour en savoir plus.
- **Abandon de la fonctionnalité SAMLv1** : la prise en charge de SAMLv1 est abandonnée.

- **Suppression du chiffrement à faible sécurité dans l'ASA 9.15(1) :** la prise en charge des chiffrements moins sécurisés suivants utilisés par IKE et IPsec a été supprimée :
  - Groupes Diffie-Hellman : 2 et 24.
  - Algorithmes de chiffrement : DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256, NULL, ESP-3DES, ESP-DES, ESP-MD5-HMAC
  - Algorithmes de hachage : MD5

Remarque Les chiffrements SSH et SSL de faible sécurité n'ont pas encore été supprimés.

Avant de passer d'une version antérieure de l'ASA à la version 9.15(1), vous devez mettre à jour votre configuration VPN afin d'utiliser les algorithmes de chiffrement pris en charge dans la version 9.15(1), faute de quoi l'ancienne configuration sera rejetée. Lorsque la configuration est rejetée, l'une des actions suivantes se produit, selon la commande :

- La commande utilisera le chiffrement par défaut.
- La commande sera supprimée.

Il est particulièrement important d'appliquer un correctif à votre configuration avant la mise à niveau pour les déploiements de mise en grappe ou de basculement. Par exemple, si l'unité secondaire est mise à niveau vers la version 9.15(1) et que les chiffrements supprimés sont synchronisés avec cette unité à partir de l'unité principale, l'unité secondaire rejettera la configuration. Ce rejet peut entraîner un comportement imprévu, comme l'impossibilité de rejoindre la grappe.

IKEv1 : les sous-commandes suivantes sont supprimées :

- **crypto ikev1 policy** *priority*:
  - **hash md5**
  - **encryption 3des**
  - **encryption des**
  - **group 2**

IKEv2 : les sous-commandes suivantes sont supprimées :

- **crypto ikev2 policy** *priority*:
  - **prf md5**
  - **integrity md5**
  - **group 2**
  - **group 24**
  - **encryption 3des**
  - **encryption des**
  - **encryption null**

IPsec : les sous-commandes suivantes sont supprimées :

- **crypto ipsec ikev1 transform-set *name* esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal *name***
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile *name***
  - **set pfs group2 group24**

Carte de chiffrement : les sous-commandes suivantes sont supprimées :

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**

- **Réintroduction de la configuration du point de distribution CRL** : l'option de configuration de l'URL statique du CDP, qui a été supprimée dans la version 9.13(1), a été réintroduite dans la commande **match-certificate**.
- **Option de restauration des contrôles de validité du certificat de contournement** : l'option de contournement de la vérification de la révocation en raison de problèmes de connectivité avec le serveur CRL ou OCSP a été restaurée.

  Les sous-commandes suivantes ont été restaurées :

  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

Directives sur 9.14

- **Prise en charge des images signées ASDM dans la version 9.14(4.14)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)
- **Échec de l'assistant de mise à niveau ASDM Cisco.com sur le Firepower 1000 et 2100 en mode appareil** : l'assistant de mise à niveau ASDM Cisco.com ne permet pas d'effectuer de mise à niveau vers la version 9.14 (**Outils > Vérifier la présence de mises à jour ASA/ASDM**). L'assistant peut mettre à niveau ASDM de la version 7.13 à la version 7.14, mais la mise à niveau de l'image ASA est grisée. (CSCvt72183) Comme solution de contournement, utilisez l'une des méthodes suivantes :

  - Utilisez **Outils > Mettre à niveau le logiciel à partir de l'ordinateur local** pour ASA et ASDM. Notez que l'image ASDM (7.14(1)) dans l'ensemble 9.14(1) comporte également le bogue CSCvt72183. Vous devez télécharger la nouvelle image 7.14(1.46) pour assurer le bon fonctionnement de l'assistant.
  - Utilisez **Outils > Vérifier la présence de mises à jour ASA/ASDM** pour procéder à la mise à niveau vers ASDM 7.14 (la version sera 7.14(1.46)). Utilisez ensuite le nouveau ASDM pour mettre à niveau l'image ASA. Notez que l'erreur **Erreur d'installation fatale** pourrait s'afficher. Dans ce cas, cliquez sur **OK**. Il convient alors de définir l'image de démarrage à l'écran **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** (Configuration, Gestion des appareils, Image/Configuration du système, Image/Configuration de démarrage). Enregistrez la configuration et rechargez l'ASA.

- **Pour les paires de basculements en version 9.14(1) ou toute version ultérieure, l'ASA ne partage plus les données du moteur client SNMP avec son homologue.**
- **Aucune prise en charge dans ASA 9.14(1) ni toute version ultérieure pour les OID cnatAddrBindNumberOfEntries et cnatAddrBindSessionCount (**CSCv22526**)**.
- **Problème de mise à niveau pour les problèmes liés à la version 9.14(4)24 et à RADIUS pour les utilisateurs mobiles AnyConnect** : pour restaurer la fonctionnalité RADIUS, procédez à une mise à niveau vers la version 9.18(4)22 ou une version ultérieure.
- **Mise à niveau du Firepower 2100 en mode plateforme** : lorsque vous effectuez une mise à niveau vers la version 9.14 ou une version ultérieure, si votre EtherChannel (port-canal) a été désactivé au moment de la mise à niveau, vous devrez activer manuellement l'EtherChannel et ses interfaces membres après la mise à niveau.
- **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)
- **Le mot clé tls-proxy et la prise en charge de l'inspection chiffrée SCCP/Skinny ont été supprimés** de la commande **inspect skinny**.
- **Assistant de mise à niveau ASDM** : en raison d'une modification interne, l'assistant est uniquement pris en charge par ASDM 7.10(1) ou les versions ultérieures. De plus, en raison d'une modification de nom d'image, vous devez utiliser ASDM 7.12(1) ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.10(1) ou une version ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM, quelle que soit la version d'ASA que vous utilisez. Veuillez noter que les ASDM 7.13 et 7.14 ne prenaient pas en charge les ASA 5512-X, 5515-X, 5585-X ou ASASM. Vous devez effectuer une mise à niveau vers ASDM 7.13(1.101) ou 7.14(1.48) pour rétablir la prise en charge d'ASDM.

Directives sur 9.13

- **ASAv nécessite une mémoire de 2 Go dans la version 9.13(1) et les versions ultérieures**. À compter de la version 9.13(1), la mémoire minimale requise pour l'ASAv est de 2 Go. Si votre instance d'ASAv actuelle fonctionne avec moins de 2 Go de mémoire, vous ne pouvez pas effectuer de mise à niveau vers la version 9.13(1) à partir d'une version antérieure. Vous devez régler la taille de la mémoire avant la mise à niveau. Consultez le guide de démarrage pour ASAv pour en savoir plus sur les allocations de ressources (vCPU et mémoire) prises en charge dans la version 9.13(1).
- **Problème de rétrogradation du Firepower 2100 en mode plateforme à partir de la version 9.13 à la version 9.12 ou à une version antérieure** : pour un Firepower 2100 disposant d'une nouvelle installation de la version 9.13 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, 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 à partir d'une version antérieure. Seules les nouvelles installations sont concernées, comme un nouveau périphérique ou un périphérique recréé. (CSCvr19755)
- **Modification de la MTU de la liaison de commande de grappe dans la version 9.13(1)** : à partir de la version 9.13(1), de nombreux paquets de contrôle de grappe sont plus volumineux que dans les versions précédentes. La MTU recommandée pour le lien de contrôle de grappe a toujours été de 1 600 ou plus, et cette valeur est appropriée. Cependant, si vous définissez la MTU à 1 600, mais que vous n'avez pas réussi à faire correspondre la MTU aux commutateurs de connexion (par exemple, vous avez laissé la MTU à 1 500 sur le commutateur), vous commencerez à voir les effets de cette incompatibilité avec les paquets de contrôle de grappe abandonnés. Assurez-vous de définir tous les périphériques de la liaison de commande de grappe sur la même MTU, soit 1 600 ou plus.
- **À partir de la version 9.13(1), l'ASA établit une connexion LDAP/SSL uniquement si l'un des critères de certification suivants est satisfait** :
  - Le certificat du serveur LDAP est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA) et est valide.
  - Un certificat d'autorité de certification des serveurs émettant la chaîne est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA), et tous les certificats d'autorité de certification subordonnés de la chaîne sont complets et valides.
- **Le serveur local de l'autorité de certification est supprimé dans la version 9.13(1)** : lorsque l'ASA est configuré en tant que serveur local d'autorité de certification, il est en mesure d'émettre des certificats numériques, de publier des listes de révocation de certificats (CRL) et de révoquer en toute sécurité les certificats émis. Cette fonctionnalité a été abandonnée et, par conséquent, la commande **crypto ca server** a été supprimée.
- **Suppression des commandes des points de distribution de la CRL** : les commandes de configuration d'URL statique du CDP, à savoir **crypto-ca-trustpoint crl** et **crl url**, ont été supprimées avec d'autres logiques connexes. L'URL du CDP a été déplacée pour correspondre à la commande de certificat.

Remarque La configuration de l'URL du CDP a été améliorée pour permettre plusieurs instances du remplacement du CDP pour une seule carte (consultez le bogue CSCvul05216).

- **Option de suppression des contrôles de validité du certificat de contournement** : l'option de contournement de la vérification de la révocation en raison de problèmes de connectivité avec le serveur CRL ou OCSP a été supprimée.

  Les sous-commandes suivantes sont supprimées :

  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

  Ainsi, après une mise à niveau, toute commande revocation-check qui n'est plus prise en charge passera au nouveau comportement en ignorant le caractère de fin none.

Remarque Ces commandes ont été restaurées ultérieurement (consultez le bogue CSCtb41710).

- **Abandon du chiffrement à faible sécurité** : plusieurs chiffrements utilisés par les modules ASA IKE, IPsec et SSH sont considérés comme étant non sécurisés et ont donc été abandonnés. Ils seront supprimés dans une version ultérieure.

  IKEv1 : les sous-commandes suivantes sont abandonnées :

  - **crypto ikev1 policy** *priority*:
    - **hash md5**
    - **encryption 3des**
    - **encryption des**
    - **group 2**
    - **group 5**

  IKEv2 : les sous-commandes suivantes sont abandonnées :

  - **crypto ikev2 policy** *priority*
    - **integrity md5**
    - **prf md5**
    - **group 2**
    - **group 5**
    - **group 24**
    - **encryption 3des**
    - **encrypted des** (cette commande est toujours disponible uniquement lorsque vous disposez de la licence de chiffrement DES)

- **encryption null**

IPsec : les commandes suivantes sont abandonnées :

- **crypto ipsec ikev1 transform-set *name* esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal *name***
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile *name***
  - **set pfs group2 group5 group24**

SSH : Les commandes suivantes sont abandonnées :

- **ssh cipher integrity custom hmac-sha1-96:hmac-md5: hmac-md5-96**
- **ssh key-exchange group dh-group1-sha1**

SSL : Les commandes suivantes sont abandonnées :

- **ssl dh-group group2**
- **ssl dh-group group5**
- **ssl dh-group group24**

Carte de chiffrement : les commandes suivantes sont abandonnées :

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group5**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group5**

- **Dans la version 9.13(1), le groupe Diffie-Hellman 14 est maintenant la valeur par défaut** pour la commande **group** sous **crypto ikev1 policy**, **ssl dh-group** et **crypto ikev2 policy**pour IPsec PFS à l'aide de **crypto map set pfs**, **crypto ipsec profile**, **crypto dynamic-map set pfs** et **crypto map set ikev1 phase1-mode**. L'ancien groupe Diffie-Hellman par défaut était le groupe 2.

  Lors de la mise à niveau à partir d'une version antérieure à la version 9.13(1), si vous devez utiliser l'ancienne valeur par défaut (Groupe Diffie-Hellman 2), vous devez configurer *manuellement* le groupe DH en tant que **groupe 2**, sans quoi vos tunnels passeront par défaut au groupe 14. Comme le groupe 2 sera supprimé dans une version ultérieure, vous devez déplacer vos tunnels dans le groupe 14 dès que possible.

Directives sur 9.12

- **Prise en charge des images signées ASDM dans la version 9.12(4.50)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco.

Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)

- Assistant de mise à niveau ASDM : en raison d'une modification interne, l'assistant est uniquement pris en charge par ASDM 7.10(1) ou les versions ultérieures. De plus, en raison d'une modification de nom d'image, vous devez utiliser ASDM 7.12(1) ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.10(1) ou une version ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM, quelle que soit la version d'ASA que vous utilisez.
- Améliorations de sécurité SSH et nouvelles valeurs par défaut dans la version 9.12(1) : consultez les améliorations de sécurité SSH suivantes :
  - La version 1 du protocole SSH n'est plus prise en charge; seule la version 2 est prise en charge. La commande **ssh version 1** sera migrée vers **ssh version 2**.
  - Prise en charge de l'échange de clés SHA256, groupe Diffie-Hellman 14. Il s'agit désormais du paramètre par défaut (**ssh key-exchange group dh-group14-sha256**). L'ancienne valeur par défaut était le groupe 1 SHA1. Assurez-vous que votre client SSH prend en charge le groupe Diffie-Hellman SHA256 14. Si ce n'est pas le cas, une erreur de ce type pourrait s'afficher :« Impossible de convenir d'un algorithme d'échange de clés ». Par exemple, l'outil OpenSSH prend en charge le groupe Diffie-Hellman 14 SHA256.
  - Prise en charge du chiffrement d'intégrité HMAC-SHA256. La valeur par défaut est désormais l'ensemble de chiffrements à haute sécurité (hmac-sha1 et hmac-sha2-256, comme défini par la commande **ssh cipher integrity high**). L'ancienne valeur par défaut était l'ensemble moyen.
- Le chiffrement NULL-SHA TLSv1 est abandonné et supprimé dans la version 9.12(1) : étant donné que NULL-SHA n'offre pas de chiffrement et n'est plus considéré comme étant sécurisé contre les menaces modernes, il sera supprimé lors du recensement des chiffrements pris en charge pour TLSv1 dans la sortie des commandes/options du mode **tls-proxy** et **show ssl ciphers all**. Les commandes **ssl cipher tlsv1 all** et **ssl cipher tlsv1 custom NULL-SHA** seront également obsolètes et supprimées.
- Le groupe de confiance par défaut est supprimé dans la version 9.12(1) : afin de se conformer à l'exigence de PSB, SEC-AUT-DEFROOT, l'ensemble d'autorités de certification de confiance « par défaut » est supprimé de l'image ASA. Par conséquent, les commandes **crypto ca trustpool import default** et **crypto ca trustpool import clean default** sont également supprimées, ainsi que les autres logiques connexes. Cependant, dans les déploiements existants, les certificats qui ont été précédemment importés à l'aide de ces commandes resteront présents.
- La commande **ssl encryption** est supprimée dans la version 9.12(1) : dans la version 9.3(2), l'abandon de la commande a été annoncé et celle-ci a été remplacée par **ssl cipher**. Dans 9.12(1), **ssl encryption** est supprimé et n'est plus pris en charge.

Directives sur 9.10

- En raison d'une modification interne, l'assistant de mise à niveau ASDM est uniquement pris en charge par ASDM 7.10(1) ou les versions ultérieures. De plus, en raison d'une modification de nom d'image, vous devez utiliser ASDM 7.12(1) ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.10(1) ou une version ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM, quelle que soit la version d'ASA que vous utilisez.

Directives sur 9.9

- Problèmes de mémoire ASA 5506-X avec de grandes configurations sur la version 9.9(2) et les versions ultérieures : si vous effectuez une mise à niveau vers la version 9.9(2) ou une version ultérieure, des parties d'une très grande configuration peuvent être rejetées en raison d'une mémoire insuffisante en présentant le message suivant : « ERREUR : mémoire insuffisante pour installer les règles ». Une option consiste à saisir la commande **object-group-search access-control** pour améliorer l'utilisation de la mémoire pour les listes de contrôle d'accès. Cependant, vos performances risquent d'en pâtir. Sinon, vous pouvez rétrograder le périphérique à la version 9.9(1).

Directives sur 9.8

- **Prise en charge des images signées ASDM dans la version 9.8(4.45)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)
- Avant la mise à niveau vers la version 9.8(2) ou une version ultérieure, le mode FIPS exige que la clé de basculement comporte au moins 14 caractères. Avant de procéder à la mise à niveau vers la version 9.8(2) ou une version ultérieure en mode FIPS, vous devez modifier le **failover key** ou le **failover ipsec pre-shared-key** pour être à au moins 14 caractères. Si votre clé de basculement est trop courte, lorsque vous mettez à niveau la première unité, la clé de basculement sera rejetée, et les deux unités deviendront actives jusqu'à ce que vous définissiez la clé de basculement à une valeur valide.
- Ne mettez pas à niveau ASAv vers la version 9.8(1) sur Amazon Web Services : en raison du bogue CSCve56153, il est conseillé de ne pas effectuer la mise à niveau vers la version 9.8(1). Après la mise à niveau, l'ASAv devient inaccessible. Passez plutôt à la version 9.8(1.5) ou à une version ultérieure.

Directives sur 9.7

- Problème de mise à niveau de la version 9.7(1) à la version 9.7(1.x) ou tout version ultérieure pour VTI et VXLAN VNI : si vous configurez à la fois Virtual Tunnel Interface (VTI) et des interfaces VNI (Virtual Network Identifier), vous ne pouvez pas effectuer de mise à niveau sans temps d'arrêt pour le basculement. Les connexions sur ces types d'interfaces ne seront pas répliquées sur l'unité de secours tant que les deux unités n'utiliseront pas la même version. (CSCvc83062)

Directives sur 9.6

- (d'ASA 9.6(2) à ASA 9.7(x)) Incidence sur la mise à niveau lors de l'utilisation de l'authentification par clé publique SSH : en raison des mises à jour de l'authentification SSH, une configuration supplémentaire est requise pour activer l'authentification par clé publique SSH; par conséquent, les configurations SSH existantes utilisant l'authentification par clé publique ne fonctionnent plus après la mise à niveau. L'authentification par clé publique est la valeur par défaut pour l'ASAv sur Amazon Web Services (AWS), donc les utilisateurs AWS verront ce problème. Pour éviter la perte de connectivité SSH, vous pouvez mettre à jour votre configuration *avant* d'effectuer la mise à niveau. Vous pouvez également utiliser ASDM après la mise à niveau (si vous avez activé l'accès ASDM) pour corriger la configuration.

Remarque Le comportement d'origine a été restauré dans la version 9.8(1).

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

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

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

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

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

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

```
username admin privilege 15
```

- Incidence sur la mise à niveau lors de la mise à niveau de l'ASA sur le Firepower 9300. En raison de modifications de nom des droits de licence sur le serveur principal, lors de la mise à niveau vers l'ASA 9.6(1)/FXOS 1.1(4), la configuration de démarrage peut ne pas être analysée correctement lors du rechargement initial; la configuration qui correspond aux droits du module complémentaire est alors rejetée.

  Pour un ASA autonome, après le rechargement de l'unité avec la nouvelle version, attendez que tous les droits soient traités et présentent l'état « Autorisé » (**afficher toutes les licences** ou **Surveillance > Propriétés > Licence Smart**), puis rechargez simplement (**recharger** ou **Outils > Rechargement du système**) *sans* enregistrer la configuration. Après le rechargement, la configuration de démarrage sera analysée correctement.

  Pour une paire de basculements, si vous disposez de droits complémentaires, suivez la procédure de mise à niveau dans les notes de mise à jour de FXOS, mais réinitialisez le basculement après avoir rechargé chaque unité (**failover reset** ou **Surveillance > Propriétés > Basculement > État**, **Surveillance > Basculement > Système**, ou **Surveillance > Basculement > Groupe de basculement**, puis cliquez sur **Réinitialiser le basculement**).

  Pour une grappe, suivez la procédure de mise à niveau dans les notes de mise à jour de FXOS; aucune autre action n'est requise.

Directives et migration sur 9.5

- 9.5(2) Nouvelle licence de transporteur : la nouvelle licence de transporteur remplace la licence GTP/GPRS existante et comprend également la prise en charge de l'inspection SCTP et Diameter. Pour le module de sécurité ASA Firepower 9300, la commande **feature mobile-sp** migrera automatiquement vers la commande **feature carrier**.
- 9.5(2) Commandes de mandataire pour courriels abandonnées : dans la version 9.5(2), les commandes de mandataire pour courriels (**imap4s**, **pop3s** et **smtps**) et les sous-commandes ne sont plus prises en charge.
- 9.5(2) Commandes CSD abandonnées ou migrées : dans la version 9.5(2), les commandes CSD (**csd image**, **show webvpn csd image**, **show webvpn csd**, **show webvpn csd hostscan** et **show webvpn csd hostscan image**) ne sont plus prises en charge.

  Les commandes CSD suivantes seront migrées : **csd enable** migre vers **hostscan enable**; **csd hostscan image** migre vers **hostscan image**.
- 9.5(2) Certaines commandes AAA avandonnées : dans la version 9.5(2) de l'ASA, ces commandes et sous-commandes AAA (**override-account-disable** et **authentication crack**) ne sont plus prises en charge.
- 9.5(1) Nous avons abandonné la commande suivante : **timeout gsn**
- Problème de mise à niveau des ASA 5508-X et 5516-X lors de la mise à niveau vers la version 9.5(x) ou une version ultérieure : avant d'effectuer la mise à niveau vers la version ASA 9.5(x) ou une version ultérieure, si vous n'avez jamais activé la réservation de trames étendues, vous devez vérifier l'empreinte mémoire maximale. En raison d'un défaut de fabrication, une limite de mémoire logicielle incorrecte a peut-être été appliquée. Si vous effectuez la mise à niveau vers la version 9.5(x) ou une version ultérieure avant d'appliquer le correctif ci-dessous, votre périphérique plantera au démarrage. Dans ce cas, vous devez rétrograder à la version 9.4 à l'aide de ROMMON (charger une image pour la gamme ASA 5500-X à l'aide de ROMMON), effectuer la procédure ci-dessous, puis effectuer de nouveau la mise à niveau.

  1. Entrez la commande suivante pour vérifier la condition de défaillance :

     ```
     ciscoasa# show memory detail | include Max memory footprint
     Max memory footprint        =    456384512
     Max memory footprint        =            0
     Max memory footprint        =    456384512
     ```

     Si une valeur inférieure à **456 384 512** est renvoyée pour « Empreinte de mémoire maximale », la condition de défaillance est présente, et vous devez effectuer les étapes restantes avant d'effectuer la mise à niveau. Si la mémoire affichée est de 456 384 512 ou plus, vous pouvez ignorer le reste de cette procédure et la mettre à niveau comme d'habitude.

  2. Accédez au mode de configuration globale :

     ```
     ciscoasa# configure terminal
     ciscoasa(config)#
     ```

  3. Activez temporairement la réservation de trames étendues :

     ```
     ciscoasa(config)# jumbo-frame reservation
     WARNING: This command will take effect after the running-config
     is saved and the system has been rebooted. Command accepted.
     ```

```
INFO: Interface MTU should be increased to avoid fragmenting
jumbo frames during transmit
```

Remarque Ne rechargez pas l'ASA.

4. Enregistrez la configuration :

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5. Désactivez la réservation de trame étendue :

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```

Remarque Ne rechargez pas l'ASA.

6. Enregistrez de nouveau la configuration :

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7. Vous pouvez maintenant effectuer une mise à niveau vers la version 9.5(x) ou une version ultérieure.

Directives et migration sur 9.4

- 9.4(1) Le mandataire du téléphone des communications unifiées et le mandataire du moteur de médias interentreprises sont abandonnés. Dans la version 9.4 de l'ASA, les mandataires du téléphone et le mandataire du moteur de médias interentreprises ne sont plus pris en charge.

Directives et migration sur 9.3

- 9.3(2) Prise en charge de la version 1.2 du protocole Transport Layer Security (TLS) : nous prenons désormais en charge la version 1.2 du protocole TLS pour la transmission sécurisée des messages pour ASDM, Clientless SSVPN et AnyConnect VPN. Nous avons introduit ou modifié les commandes suivantes : ssl client-version, ssl server-version, ssl cipher, ssl trust-point et ssl dh-group. Nous avons abandonné la commande suivante : ssl encryption
- 9.3(1) Suppression de l'authentification de domaine AAA Windows NT : nous avons supprimé la prise en charge de NTLM pour les utilisateurs de VPN d'accès à distance. Nous avons abandonné la commande suivante : aaa-server protocol nt

Directives et migration sur 9.2

Vérification du certificat du serveur de mise à jour automatique

9.2(1) Vérification du certificat du serveur de mise à jour automatique activée par défaut. 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 :

```
AVERTISSEMENT : Le certificat fourni par les serveurs de mise à jour automatique ne sera
pas vérifié. Pour vérifier ce certificat, utilisez l'option avec le certificat de
vérification.
```

La configuration sera migrée vers la configuration explicite sans vérification :

auto-update server no-verification

Incidence sur la mise à niveau pour la connexion à ASDM

Incidence sur la mise à niveau pour la connexion à ASDM lors de la mise à niveau d'une version antérieure à la version 9.2(2.4) à la version 9.2(2.4), ou toute version ultérieure. Si vous effectuez une mise à niveau d'une version antérieure à la version 9.2(2.4) vers la version 9.2(2.4) d'ASA ou une version ultérieure et que vous utilisez l'autorisation de commande et les rôles d'utilisateur définis par ASDM, les utilisateurs avec un accès en lecture seule ne pourront pas se connecter à ASDM. Vous devez modifier la commande **more** avant ou après la mise à niveau pour être au niveau de privilège 5; seuls les utilisateurs de niveau Administrateur peuvent apporter cette modification. Veuillez noter que la version 7.3(2) et les versions ultérieures d'ASDM comprend la commande **more** au niveau 5 pour les rôles d'utilisateur définis, mais les configurations préexistantes doivent être corrigées manuellement.

ASDM :

1. Choisissez **Configuration > Gestion des périphériques > Utilisateurs/AAA > Accès AAA > Autorisation**, puis cliquez sur **Configurer les privilèges de commande**.
2. Sélectionnez **Plus**, puis cliquez sur **Modifier**.

3. Définissez le **niveau de privilège** sur 5 et cliquez sur **OK**.
4. Cliquez sur **OK**, puis sur **Appliquer**.

Interface de ligne de commande :

```
ciscoasa(config)# privilege cmd level 5 mode exec command more
```

Directives et migration sur 9.1

- La MTU maximale est maintenant de 9 198 octets : si votre MTU a été définie à une valeur supérieure à 9 198, la MTU est automatiquement réduite lors de la mise à niveau. Dans certains cas, cette modification de la MTU peut entraîner une non-concordance de la MTU. Assurez-vous de configurer tout équipement de connexion pour utiliser la nouvelle valeur MTU. La MTU maximale que l'ASA peut utiliser est de 9 198 octets (vérifiez la limite exacte de votre modèle à l'aide de l'interface de ligne de commande).

Cette valeur n'inclut pas l'en-tête de couche 2. L'ASA vous a permis de définir une MTU maximale de 65 535 octets, ce qui était inexact et pourrait causer des problèmes.

Directives et migration sur 9.0

- **Migration des listes de contrôle d'accès IPv6** : les listes de contrôle d'accès IPv6 (**ipv6 access-list**) seront migrées vers les listes de contrôle d'accès étendues (**access-list extended**); les listes de contrôle d'accès IPv6 ne sont plus prises en charge.

  Si les listes de contrôle d'accès IPv4 et IPv6 sont appliquées dans la même direction d'une commande d'interface (**access-group**), les listes de contrôle d'accès sont fusionnées :

  - Si les listes de contrôle d'accès IPv4 et IPv6 ne sont utilisées nulle part ailleurs que dans le groupe d'accès, le nom de la liste de contrôle d'accès IPv4 est utilisé pour la liste de contrôle d'accès fusionnée; la liste de contrôle d'accès IPv6 est supprimée.
  - Si au moins une des listes de contrôle d'accès est utilisée dans une autre fonctionnalité, une nouvelle liste de contrôle d'accès est créée avec le nom *IPv4-ACL-name_IPv6-ACL-name*. La ou les listes de contrôle d'accès en cours d'utilisation continuent d'être utilisées pour d'autres fonctionnalités. Les listes de contrôle d'accès qui ne sont pas utilisées sont supprimées. Si la liste de contrôle d'accès IPv6 est utilisée pour une autre fonctionnalité, elle est migrée vers une liste de contrôle d'accès étendue du même nom.

- **Migration du mot clé « tout » de la liste de contrôle d'accès** : maintenant que les listes de contrôle d'accès prennent en charge les protocoles IPv4 et IPv6, le mot clé **any** représente désormais « tout le trafic IPv4 et IPv6 ». Toutes les listes de contrôle d'accès existantes qui utilisent le mot clé **any** seront modifiées pour utiliser le mot clé **any4**, qui désigne « tout le trafic IPv4 ».

  En outre, un mot clé distinct a été introduit pour désigner « tout le trafic IPv6 » : **any6**.

  Les mots clés **any4** et **any6** ne sont pas disponibles pour toutes les commandes qui utilisent le mot clé **any**. Par exemple, la fonctionnalité NAT utilise uniquement le mot clé **any**; le mot clé « tout » représente le trafic IPv4 ou le trafic IPv6 selon le contexte dans la commande NAT en particulier.

- **Exigences en matière de NAT statique avec traduction de port avant la mise à niveau** : dans la version 9.0 et les versions ultérieures, les règles statiques de NAT avec traduction de port limitent l'accès à l'adresse IP de destination pour le port spécifié uniquement. Si vous essayez d'accéder à l'adresse IP de destination sur un port différent non couvert par une règle NAT, la connexion est bloquée. Ce comportement est également valable pour la NAT Twice. De plus, le trafic qui ne correspond pas à l'adresse IP source de la règle NAT Twice sera abandonné s'il correspond à l'adresse IP de destination, quel que soit le port de destination. Par conséquent, avant de procéder à la mise à niveau, vous devez ajouter des règles supplémentaires pour tout autre trafic autorisé vers l'adresse IP de destination.

  Par exemple, la règle NAT Object suivante permet de traduire le trafic HTTP vers le serveur interne entre le port 80 et le port 8080 :

  ```
  object network my-http-server
    host 10.10.10.1
    nat (inside,outside) static 192.168.1.1 80 8080
  ```

  Si vous souhaitez que d'autres services puissent atteindre le serveur, comme FTP, vous devez les autoriser explicitement :

  ```
  object network my-ftp-server
  ```

```
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1 ftp ftp
```

Ou, pour autoriser le trafic vers d'autres ports du serveur, vous pouvez ajouter une règle NAT statique générale qui correspondra à tous les autres ports :

```
object network my-server-1
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1
```

Pour la NAT Twice, la règle suivante permet d'autoriser le trafic HTTP de l'adresse 192.168.1.0/24 vers le serveur interne et de le traduire entre le port 80 et le port 8080 :

```
object network my-real-server
  host 10.10.10.1
object network my-mapped-server
  host 192.168.1.1
object network outside-real-hosts
  subnet 192.168.1.0 255.255.255.0
object network outside-mapped-hosts
  subnet 10.10.11.0 255.255.255.0
object service http-real
  service tcp destination eq 80
object service http-mapped
  service tcp destination eq 8080
object service ftp-real
  service tcp destination eq 21
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server service http-mapped http-real
```

Si vous souhaitez que les hôtes externes atteignent un autre service sur le serveur interne, ajoutez une autre règle NAT pour le service, par exemple FTP :

```
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server ftp-real ftp-real
```

Si vous souhaitez que d'autres adresses sources atteignent le serveur interne sur tous les autres ports, vous pouvez ajouter une autre règle NAT pour cette adresse IP spécifique ou pour n'importe quelle adresse IP source. Assurez-vous que la règle générale est classée après la règle spécifique.

```
nat (outside,inside) source static any any destination static my-mapped-server
my-real-server
```

Directives et migration sur 8.4

- Migration de la configuration pour le mode transparent : dans la version 8.4, toutes les interfaces en mode transparent appartiennent désormais à un groupe de ponts. Lors de la mise à niveau vers la version 8.4, les deux interfaces existantes sont placées dans le groupe de ponts 1, et l'adresse IP de gestion est attribuée à la BVI (Bridge Group Virtual Interface). La fonctionnalité reste la même lors de l'utilisation d'un groupe de ponts. Vous pouvez désormais profiter de la fonctionnalité de groupe de ponts pour configurer jusqu'à quatre interfaces par groupe de ponts et créer jusqu'à huit groupes de ponts en mode unique ou par contexte.

Remarque Remarque : Dans la version 8.3 et les versions antérieures, en tant que configuration non prise en charge, vous pourriez configurer une interface de gestion sans adresse IP et vous pourriez accéder à l'interface en utilisant l'adresse de gestion des périphériques. Dans la version 8.4, l'adresse de gestion des périphériques est attribuée aux BVI, et l'interface de gestion n'est plus accessible en utilisant cette adresse IP; l'interface de gestion nécessite sa propre adresse IP.

- Lors de la mise à niveau vers la version 8.4(2) à partir des versions 8.3(1), 8.3(2) et 8.4(1), toutes les configurations NAT d'identité incluront désormais les mots clés **no-proxy-arp** et **route-lookup** pour maintenir les fonctionnalités existantes. Le mot clé **unidirectional** est supprimé.

Directives et migration sur 8.3

Consultez le guide suivant qui décrit le processus de migration de la configuration lorsque vous passez d'une version antérieure à la version 8.3 du système d'exploitation Cisco ASA 5500 à la version 8.3 :

Migration du Cisco ASA 5500 vers la version 8.3

Directives de mise en grappe

Il n'y a aucune exigence particulière pour les mises à niveau sans temps d'arrêt pour la mise en grappe ASA, avec les exceptions suivantes.

Remarque *Les rétrogradations* sans temps d'arrêt ne sont pas officiellement prises en charge par la mise en grappe.

- Exigences de mise à niveau transparente du basculement et de la mise en grappe du Firepower 4100/9300 pour le déchargement de flux : en raison de corrections de bogues dans la fonction de déchargement de flux, certaines combinaisons de FXOS et d'ASA ne prennent pas en charge le déchargement de flux (consultez le tableau de compatibilité). Le déchargement de flux est désactivé par défaut pour l'ASA. Pour effectuer une mise à niveau transparente du basculement ou de la mise en grappe lors de l'utilisation du déchargement de flux, vous devez suivre les chemins de mise à niveau ci-dessous pour vous assurer d'exécuter toujours une combinaison compatible lors de la mise à niveau vers FXOS 2.3.1.130 ou une version ultérieure :

  1. Mettre à niveau l'ASA vers la version 9.8(3) ou une version ultérieure
  2. Mettre à niveau FXOS vers la version 2.3.1.130 ou une version ultérieure
  3. Mettre à niveau l'ASA vers votre version finale

  Par exemple, vous utilisez FXOS 2.2.2.26/ASA 9.8(1) et vous souhaitez effectuer une mise à niveau vers FXOS 2.6.1/ASA 9.12(1), vous pouvez :

  1. Mettre à niveau l'ASA vers la version 9.8(4)
  2. Mettre à niveau FXOS vers la version 2.6.1
  3. Mettre à niveau l'ASA vers la version 9.12(1)

- Mise à niveau de la grappe Firepower 4100/9300 vers FXOS 2.3/ASA 9.9(2) : les unités de données sur ASA 9.8 ou les versions antérieures ne peuvent pas joindre une grappe dont l'unité de contrôle se trouve sur FXOS 2.3/9.9(2) ou une version ultérieure. Elles rejoindront la grappe après la mise à niveau d'ASA vers la version 9.9(2) ou toute version ultérieure [CSCvi54844].
- VPN de site à site distribué : les sessions VPN de site à site distribuées sur une unité en panne requièrent jusqu'à 30 minutes pour se stabiliser sur les autres unités. Pendant cette période, des défaillances supplémentaires de l'unité peuvent entraîner la perte de sessions. Par conséquent, lors d'une mise à niveau de grappe, pour éviter une perte de trafic, suivez ces étapes. Reportez-vous à la procédure de mise à niveau de grappe FXOS/ASA afin de pouvoir intégrer ces étapes dans votre tâche de mise à niveau.

Remarque La mise à niveau sans temps d'arrêt n'est pas prise en charge avec le VPN de site à site distribué lors de la mise à niveau de la version 9.9(1) à la version 9.9(2) ou à une version ultérieure. Dans la version 9.9(2), en raison des améliorations de la redistribution active des sessions, vous ne pouvez pas exécuter certaines unités sur la version 9.9(2) et d'autres unités sur la version 9.9(1).

1. Sur les châssis *sans* unité de contrôle, désactivez la mise en grappe sur un module à l'aide de la console ASA.

   cluster group *name*

   no enable

   Si vous mettez à niveau FXOS sur le châssis ainsi que sur l'ASA, enregistrez la configuration pour que la mise en grappe soit désactivée après le redémarrage du châssis :

   write memory

2. Attendez que la grappe se stabilise; vérifiez que toutes les sessions de sauvegarde ont bien été créées.

   show cluster vpn-sessiondb summary

3. Répétez les étapes 1 et 2 pour chaque module de ce châssis.
4. Mettez à niveau FXOS sur le châssis à l'aide de l'interface de ligne de commande de FXOS ou de Firepower Chassis Manager.
5. Une fois que le châssis est en ligne, mettez à jour l'image ASA sur chaque module à l'aide de l'interface de ligne de commande de FXOS ou de Firepower Chassis Manager.
6. Une fois que les modules sont en ligne, réactivez la mise en grappe sur chaque module sur la console de l'ASA.

   cluster group *name*

   enable

   write memory

7. Répétez les étapes 1 à 6 sur le deuxième châssis, en veillant à désactiver la mise en grappe sur les unités de données, puis sur l'unité de contrôle.

   Une nouvelle unité de contrôle sera choisie dans le châssis mis à niveau.

8. Une fois que la grappe est stable, redistribuez les sessions actives entre tous les modules de la grappe à l'aide de la console ASA sur l'unité de contrôle.

cluster redistribute vpn-sessiondb

- Problème de mise à niveau pour la version 9.9(1) et les versions ultérieures avec la mise en grappe. La version 9.9(1) et les versions ultérieures comprennent une amélioration de la distribution des sauvegardes. Vous devez effectuer votre mise à niveau vers la version 9.9(1) ou une version ultérieure comme suit pour profiter de la nouvelle méthode de distribution des sauvegardes. Dans le cas contraire, les unités mises à niveau continueront d'utiliser l'ancienne méthode.

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

- Mise à niveau de la grappe Firepower 4100/9300 vers ASA 9.8(1) ou versions antérieures : lorsque vous désactivez la mise en grappe sur une unité de données (**no enable**), qui fait partie du processus de mise à niveau, le trafic redirigé vers cette unité peut être abandonné pendant trois secondes avant que le trafic soit redirigé vers un nouveau propriétaire [CSCvc85008].

- La mise à niveau sans temps d'arrêt peut ne pas être prise en charge lors de la mise à niveau vers les versions suivantes avec le correctif pour le bogue CSCvb24585. Ce correctif a déplacé l'algorithme 3DES des chiffrements SSL par défaut (moyen) à l'ensemble de chiffrement faible. Si vous définissez un chiffrement personnalisé qui n'inclut plus l'algorithme 3DES, vous risquez d'avoir une incompatibilité si l'autre côté de la connexion utilise les algorithmes de chiffrement par défaut (moyens) qui n'incluent plus l'algorithme 3DES.
  - 9.1(7.12)
  - 9.2(4.18)
  - 9.4(3.12)
  - 9.4(4)
  - 9.5(3.2)
  - 9.6(2.4)
  - 9.6(3)
  - 9.7(1)
  - 9.8(1)

- Problèmes de mise à niveau pour les listes de contrôle d'accès de nom de domaine complet (FQDN) : en raison du bogue CSCv92371, les listes de contrôle d'accès contenant des noms de domaine complets peuvent entraîner une réplication incomplète des listes de contrôle d'accès sur les unités secondaires d'une paire de grappe ou de basculements. Ce bogue est présent dans les versions 9.1(7), 9.5(2), 9.6(1) et certaines versions provisoires. Nous vous suggérons de procéder à la mise à niveau vers une version qui comprend le correctif pour le bogue CSCuy34265 : la version 9.1(7.6) ou une version ultérieure, la version 9.5(3) ou une version ultérieure, la version 9.6(2) ou une version ultérieure. Cependant, en raison de la nature de la réplication de la configuration, la mise à niveau sans temps d'arrêt n'est pas disponible. Consultez le bogue CSCuy34265 pour en savoir plus sur les différentes méthodes de mise à niveau.

- Les grappes Firepower Threat Defense en version 6.1.0 ne prennent pas en charge la mise en grappe intersite (vous pouvez configurer les fonctionnalités intersite à l'aide de FlexConfig à partir de la version 6.2.0). Si vous avez déployé ou redéployé une grappe 6.1.0 dans FXOS 2.1.1 et que vous avez saisi une valeur pour l'ID de site (non pris en charge), vous devez supprimer l'ID de site (le définir sur **0**) sur chaque unité dans FXOS avant de passer à la version 6.2.3. Sinon, les unités ne pourront pas rejoindre la grappe après la mise à niveau. Si vous avez déjà effectué la mise à niveau, modifiez l'ID de site à **0** sur chaque unité pour résoudre le problème. Consultez le guide de configuration de FXOS pour afficher ou modifier l'ID de site
- Mise à niveau vers la version 9.5(2) ou une version ultérieure (CSCuv82933) : avant de mettre à niveau l'unité de contrôle, si vous saisissez **show cluster info**, les unités de données mises à niveau s'affichent comme « DEPUTY_BULK_SYNC ». D'autres états de non-concordance s'affichent également. Vous pouvez ignorer cet affichage; l'état s'affichera correctement lorsque vous mettrez à niveau toutes les unités.
- Mise à niveau à partir de la version 9.0(1) ou de la version 9.1(1) (CSCue72961) : la mise à niveau sans temps d'arrêt n'est pas prise en charge.

Directives en matière de basculement

Il n'y a aucune exigence particulière concernant les mises à niveau sans temps d'arrêt pour le basculement, avec les exceptions suivantes :

- Pour le Firepower 1010, la présence d'identifiants de VLAN non valides peuvent causer des problèmes.Avant d'effectuer une mise à niveau vers la version 9.15(1), assurez-vous de ne pas utiliser de VLAN pour les ports de commutation de la plage de 3968 à 4047. Ces identifiants sont pour un usage interne uniquement, et la version 9.15(1) comprend une vérification pour vous assurer de ne pas utiliser ces identifiants. Par exemple, si ces identifiants sont utilisés après la mise à niveau d'une paire de basculements, la paire de basculements passera à l'état suspendu. Consultez le bogue CSCvw33057 pour en savoir plus.
- Exigences de mise à niveau transparente du basculement et de la mise en grappe du Firepower 4100/9300 pour le déchargement de flux : en raison de corrections de bogues dans la fonction de déchargement de flux, certaines combinaisons de FXOS et d'ASA ne prennent pas en charge le déchargement de flux (consultez le tableau de compatibilité). Le déchargement de flux est désactivé par défaut pour l'ASA. Pour effectuer une mise à niveau transparente du basculement ou de la mise en grappe lors de l'utilisation du déchargement de flux, vous devez suivre les chemins de mise à niveau ci-dessous pour vous assurer d'exécuter toujours une combinaison compatible lors de la mise à niveau vers FXOS 2.3.1.130 ou une version ultérieure :

  1. Mettre à niveau l'ASA vers la version 9.8(3) ou une version ultérieure
  2. Mettre à niveau FXOS vers la version 2.3.1.130 ou une version ultérieure
  3. Mettre à niveau l'ASA vers votre version finale

  Par exemple, vous utilisez FXOS 2.2.2.26/ASA 9.8(1) et vous souhaitez effectuer une mise à niveau vers FXOS 2.6.1/ASA 9.12(1), vous pouvez :

  1. Mettre à niveau l'ASA vers la version 9.8(4)
  2. Mettre à niveau FXOS vers la version 2.6.1
  3. Mettre à niveau l'ASA vers la version 9.12(1)

- Problèmes de mise à niveau avec les versions 8.4(6), 9.0(2) et 9.1(2) : en raison du bogue CSCum88962, vous ne pouvez pas effectuer de mise à niveau sans temps d'arrêt vers les versions 8.4(6), 9.0(2) ou 9.1(3). Vous devriez plutôt passer à la version 8.4(5) ou 9.0(3). Pour mettre à niveau la version 9.1(1), vous ne pouvez pas effectuer de mise à niveau directement vers la version 9.1(3) en raison du bogue CSCuh25271. Il n'y a donc pas de solution de contournement pour une mise à niveau sans temps d'arrêt. Vous devez effectuer la mise à niveau vers la version 9.1(2) avant de procéder à la mise à niveau vers la version 9.1(3) ou toute version ultérieure.
- Problèmes de mise à niveau pour les listes de contrôle d'accès de nom de domaine complet (FQDN) : en raison du bogue CSCv92371, les listes de contrôle d'accès contenant des noms de domaine complets peuvent entraîner une réplication incomplète des listes de contrôle d'accès sur les unités secondaires d'une paire de grappe ou de basculements. Ce bogue est présent dans les versions 9.1(7), 9.5(2), 9.6(1) et certaines versions provisoires. Nous vous suggérons de procéder à la mise à niveau vers une version qui comprend le correctif pour le bogue CSCuy34265 : la version 9.1(7.6) ou une version ultérieure, la version 9.5(3) ou une version ultérieure, la version 9.6(2) ou une version ultérieure. Cependant, en raison de la nature de la réplication de la configuration, la mise à niveau sans temps d'arrêt n'est pas disponible. Consultez le bogue CSCuy34265 pour en savoir plus sur les différentes méthodes de mise à niveau.
- Problème de mise à niveau de la version 9.7(1) à la version 9.7(1.x) ou tout version ultérieure pour VTI et VXLAN VNI : si vous configurez à la fois Virtual Tunnel Interface (VTI) et des interfaces VNI (Virtual Network Identifier), vous ne pouvez pas effectuer de mise à niveau sans temps d'arrêt pour le basculement. Les connexions sur ces types d'interfaces ne seront pas répliquées sur l'unité de secours tant que les deux unités n'utiliseront pas la même version. (CSCvc83062)
- Avant la mise à niveau vers la version 9.8(2) ou une version ultérieure, le mode FIPS exige que la clé de basculement comporte au moins 14 caractères. Avant de procéder à la mise à niveau vers la version 9.8(2) ou une version ultérieure en mode FIPS, vous devez modifier le **failover key** ou le **failover ipsec pre-shared-key** pour être à au moins 14 caractères. Si votre clé de basculement est trop courte, lorsque vous mettez à niveau la première unité, la clé de basculement sera rejetée, et les deux unités deviendront actives jusqu'à ce que vous définissiez la clé de basculement à une valeur valide.
- Problème de mise à niveau avec l'inspection GTP : il pourrait y avoir un temps d'arrêt pendant la mise à niveau, car les structures de données GTP ne sont pas répliquées sur le nouveau nœud.

Directives supplémentaires

- Vulnérabilité de l'intégrité de la personnalisation du portail du VPN SSL sans client Cisco ASA : plusieurs vulnérabilités ont été corrigées pour le VPN SSL sans client dans le logiciel ASA. Vous devez donc mettre à niveau votre logiciel vers une version fixe. Consultez la page http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa pour en savoir plus sur la vulnérabilité et obtenir la liste des versions d'ASA corrigées. En outre, si vous avez déjà exécuté une version antérieure d'ASA dont la configuration était vulnérable, quelle que soit la version que vous utilisez actuellement, vous devez vérifier que la personnalisation du portail n'a pas été compromise. Si un agresseur a compromis un objet personnalisé dans le passé, l'objet compromis reste persistant après la mise à niveau de l'ASA vers une version corrigée. La mise à niveau de l'ASA empêche cette vulnérabilité d'être davantage exploitée, mais elle ne modifiera pas les objets de personnalisation qui ont déjà été compromis et qui sont toujours présents sur le système.

Directives de mise à niveau de FXOS

Avant d'effectuer la mise à niveau, lisez les notes de mise à jour pour chaque version de FXOS dans le chemin de mise à niveau de votre choix. Les notes de mise à jour contiennent des renseignements importants sur chaque version FXOS, y compris les nouvelles fonctionnalités et les fonctionnalités modifiées.

La mise à niveau peut nécessiter des modifications de la configuration que vous devez prendre en compte. Par exemple, un nouveau matériel informatique pris en charge dans une version FXOS peut également nécessiter la mise à jour du micrologiciel FXOS.

Les notes de mise à jour de FXOS sont disponibles ici : https://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html.

Liste de contrôle pour la mise à niveau d'ASA

Pour planifier votre mise à niveau, utilisez cette liste de contrôle.

1. Modèle d'ASA (Chemin de mise à niveau : Appareils ASA, à la page 45) : _____

   Version actuelle de l'ASA (Chemin de mise à niveau : Appareils ASA, à la page 45) : _____
2. Vérifiez la compatibilité ASA/ASDM par modèle (Compatibilité ASA et ASDM par modèle, à la page 25).

   Version de l'ASA cible : _____

   Version d'ASDM cible : _____
3. Vérifiez le chemin de mise à niveau du Firepower 2100 en mode plateforme (Chemin de mise à niveau : ASA sur Firepower 2100 en mode plateforme, à la page 52). Des versions intermédiaires sont-elles requises? Oui _____ Non _____

   Si tel est le cas, version(s) d'ASA intermédiaire(s) : _____
4. Téléchargez les versions d'ASA/ASDM cibles (Télécharger le logiciel ASA, à la page 61).

Remarque ASDM est inclus dans le paquet d'images pour toutes les plateformes Firepower et Cisco Secure Firewall.

5. Votre modèle ASA est-il un Firepower 4100 ou 9300? Oui _____ Non _____

   En cas de réponse positive :

   1. Version de FXOS actuelle : _____
   2. Vérifiez la compatibilité de ASA/Firepower 4100 et 9300 (Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces, à la page 33).

      Version de FXOS cible : _____
   3. Des versions intermédiaires sont-elles requises? Oui _____ Non _____

      Si oui, versions de FXOS intermédiaires : _____

      Assurez-vous de planifier la mise à niveau de l'ASA conformément aux mises à niveau de FXOS pour maintenir leur compatibilité.

Versions ASA intermédiaires requises pour maintenir la compatibilité. pendant la mise à niveau : _____

4. Téléchargez les versions de FXOS cibles et intermédiaires (Télécharger FXOS pour le Firepower 4100/9300, à la page 73).

   Téléchargez les versions d'ASA intermédiaires (Télécharger le logiciel ASA, à la page 61).

5. Utilisez-vous l'application décorateur Radware DefensePro? Oui _____ Non _____

   En cas de réponse positive :

   1. Version actuelle de DefensePro : _____
   2. Vérifiez la compatibilité de ASA/FXOS/DefensePro (Compatibilité avec Radware DefensePro, à la page 40).

      Version de Target DefensePro : _____
   3. Téléchargez la version de DefensePro cible.

6. Consultez les directives de mise à niveau pour chaque système d'exploitation.
   - Lignes directrices pour la mise à niveau de l'ASA, à la page 1.
   - Directives FXOS : consultez les notes de mise à jour FXOS pour chaque version intermédiaire et cible.

7. Sauvegardez vos configurations. Consultez le guide de configuration de chaque système d'exploitation pour connaître les méthodes de sauvegarde.

Compatibilité

Cette section comprend des tableaux indiquant la compatibilité entre les plateformes, les systèmes d'exploitation et les applications.

Compatibilité ASA et ASDM par modèle

Les tableaux suivants répertorient la compatibilité d'ASA et d'ASDM pour les modèles actuels. Pour les anciennes versions et les anciens modèles, consultez Compatibilité de Cisco ASA.

ASA 9.22

Les versions recommandées sont en **gras**.

Remarque

- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.22(1) peut gérer un ASA 5516-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.20 avec ASA 9.22. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.22(1.2) avec ASDM 7.22(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.

Tableau 1 : Compatibilité ASA et ASDM : la version 9.22

ASA	ASDM	Modèle ASA								
		ASA virtuel	Firepower 1010 1010E 1120 Série 1150	Secure Firewall 1210CE 1210CP 1220CX		Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 4225 4245	Firepower 9300	ISA 3000
9.22(1.1)	7.22(1)	**OUI**	**OUI**	**OUI**		**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

ASA 9.20 et 9.19

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.20(x) était la version finale pour la série Firepower 2100.
- ASA 9.18(x) était la version finale pour les Firepower 4110, 4120, 4140 et 4150, et les modules de sécurité SM-24, SM-36 et SM-44 pour le Firepower 9300.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.19(1) peut gérer un ASA 5516-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.18 with ASA 9.19. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.20(1.5) avec ASDM 7.20(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.

Tableau 2 : Compatibilité ASA et ASDM : de la version 9.20 à la version 9.19

ASA	ASDM	Modèle ASA								
		ASA virtuel	Firepower 1010 1120 Série 1150		Firepower de la série 2110 2120 2130 2140	Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 4225 4245	Firepower 9300	ISA 3000
9.20(3)	7.20(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.20(2)	7.20(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.20(1)	7.20(1)	—	—	—	—	—	—	**OUI**	—	—
9.19(1)	7.19(1)	**OUI**	**OUI**		**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**

ASA 9.18 à 9.17

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.16(x) était la version finale pour les ASA 5506-X, 5506H-X, 5506W-X, 5508-X et 5516-X.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.17(1) peut gérer un ASA 5516-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.17 avec ASA 9.18. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.17(1.2) avec ASDM 7.17(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.
- ASA 9.17(1.13) et 9.18(2) ou les versions ultérieures nécessitent ASDM 7.18(1.152) ou une version ultérieure. L'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une image ASDM antérieure à la version 7.18(1.152) avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. (CSCwb05291, CSCwb05264)

Tableau 3 : Compatibilité ASA et ASDM : de la version 9.18 à la version 9.17

ASA	ASDM	Modèle ASA							
		ASA virtuel	Firepower 1010 1120 Série 1150		Firepower de la série 2110 2120 2130 2140	Secure Firewall 3110 3120 3130 3140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.18(4)	7.19(1)95	**OUI**	**OUI**		**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.18(3)	7.18(1.152)	**OUI**	**OUI**		**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.18(2)	7.18(1.152)	**OUI**	**OUI**	—	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.18(1)	7.18(1)	**OUI**	**OUI**	—	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.17(1.13)	7.18(1.152)	**OUI**	**OUI**	—	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.17(1)	7.17(1.155)	**OUI**	**OUI**	—	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

ASA 9.16 à 9.15

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.16(x) était la version finale pour les ASA 5506-X, 5506H-X, 5506W-X, 5508-X et 5516-X.
- ASA 9.14(x) est la version finale pour les ASA 5525-X, 5545-X et 5555-X.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.15(1) peut gérer un ASA 5516-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.15 with ASA 9.16. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.16(1.15) avec ASDM 7.16(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.
- ASA 9.16(3.19) et les versions ultérieures nécessitent ASDM 7.18(1.152) ou une version ultérieure. L'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une image ASDM antérieure à la version 7.18(1.152) avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. (CSCwb05291, CSCwb05264)

Tableau 4 : Compatibilité ASA et ASDM : de la version 9.16 à la version 9.15

ASA	ASDM	Modèle ASA						
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASAv	Firepower 1010 1120 Série 1150	Firepower de la série 2110 2120 2130 2140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.16(4)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.16(3.19)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.16(3)	7.16(1.150)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.16(2)	7.16(1.150)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.16(1)	7.16(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.15(1)	7.15(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

ASA 9.14 à 9.13

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.14(x) est la version finale pour les ASA 5525-X, 5545-X et 5555-X.
- ASA 9.12(x) est la version finale pour les ASA 5512-X, 5515-X, 5585-X et ASASM.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.13(1) peut gérer un ASA 5516-X sur ASA 9.10(1). Les ASDM 7.13(1) et ASDM 7.14(1) ne prenaient pas en charge les ASA 5512-X, 5515-X, 5585-X et ASASM. Vous devez effectuer une mise à niveau vers ASDM 7.13(1.101) ou 7.14(1.48) pour rétablir la prise en charge d'ASDM.
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.13 avec ASA 9.14. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.14(1.2) avec ASDM 7.14(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.
- ASA 9.14(4.14) et les versions ultérieures nécessitent ASDM 7.18(1.152) ou une version ultérieure. L'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une image ASDM antérieure à la version 7.18(1.152) avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. (CSCwb05291, CSCwb05264)

Tableau 5 : Compatibilité ASA et ASDM : de la version 9.14 à la version 9.13

ASA	ASDM	Modèle ASA							
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5525-X 5545-X 5555-X	ASAv	Firepower 1010 1120 Série 1150	Firepower de la série 2110 2120 2130 2140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.14(4.14)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.14(4)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.14(3)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

ASA	ASDM	Modèle ASA							
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5525-X 5545-X 5555-X	ASAv	Firepower 1010 1120 Série 1150	Firepower de la série 2110 2120 2130 2140	Firepower4110 4112 4115 4120 4125 4140 4145 4150	Firepower9300	ISA 3000
9.14(2)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.14(1.30)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.14(1.6)	7.14(1.48)	—	—	**OUI** (+ASAv100)	—	—	—	—	—
9.14(1)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.13(1)	7.13(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI** (sauf 4112)	**OUI**	**OUI**

ASA 9.12 à 9.5

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.12(x) est la version finale pour les ASA 5512-X, 5515-X, 5585-X et ASASM.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.12(1) peut gérer un ASA 5515-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.10 avec ASA 9.12. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.12(1.15) avec ASDM 7.12(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.
- ASA 9.8(4.45) et 9.12(4.50) ou les versions ultérieures nécessitent ASDM 7.18(1.152) ou une version ultérieure. L'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une image ASDM antérieure à la version 7.18(1.152) avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. (CSCwb05291, CSCwb05264)

Tableau 6 : Compatibilité ASA et ASDM : de la version 9.12 à la version 9.5

ASA	ASDM	Modèle ASA									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower de la série 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.12(4.50)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.12(4)	7.12(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.12(3)	7.12(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.12(2)	7.12(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.12(1)	7.12(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.10(1)	7.10(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.9(2)	7.9(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.9(1)	7.9(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(4.45)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(4)	7.8(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(3)	7.8(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(2)	7.8(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(1.200)	Aucun soutien	—	—	—	**OUI**	—	—	—	—	—	—
9.8(1)	7.8(1)	**OUI**	**OUI**	**OUI**	**OUI** (+ASAv50)	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.7(1.4)	7.7(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.6(4)	7.9(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.6(3.1)	7.7(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.6(2)	7.6(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.6(1)	7.6(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI** (sauf 4 150)	—	**OUI**	**OUI**

ASA	ASDM	Modèle ASA									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower de la série 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.5(3.9)	7.6(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	—	—	—	**OUI**
9.5(2.200)	7.5(2.153)	—	—	—	**OUI**	—	—	—	—	—	—
9.5(2.2)	7.5(2)	—	—	—	—	—	—	—	—	**OUI**	—
9.5(2.1)	7.5(2)	—	—	—	—	—	—	—	—	**OUI**	—
9.5(2)	7.5(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	—	—	—	**OUI**
9.5(1.200)	7.5(1)	—	—	—	**OUI**	—	—	—	—	—	—
9.5(1.5)	7.5(1.112)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	—	—	—	—
9.5(1)	7.5(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	—	—	—	—

Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces

Pour les périphériques Firepower 4100/9300, vous devez maintenir la compatibilité entre FXOS et tous les périphériques logiques ASA et défense contre les menaces . Mettez à niveau FXOS avant de mettre à niveau le logiciel. Les versions **en gras** dans le tableau suivant sont des versions associées spécialement qualifiées (test amélioré). Utilisez ces combinaisons chaque fois que cela est possible.

Notez que pour les autres modèles de périphériques, le travail de compatibilité FXOS est effectué pour vous. Dans la plupart des cas, la mise à niveau du logiciel met automatiquement à niveau FXOS. Pour Secure Firewall 3100/4200 en mode multi-instance, le centre de gestion vous guide tout au long de la mise à niveau de FXOS, puis défense contre les menaces .

Pour mettre à niveau :

- FXOS : À partir de FXOS 2.2.2 et les versions ultérieures, vous pouvez effectuer une mise à niveau directement vers n'importe quelle version ultérieure. (FXOS 2.0.1–2.2.1 peut être mis à niveau jusqu'à la version 2.8.1. Pour les versions antérieures à la version 2.0.1, vous devez effectuer une mise à niveau à chaque version intermédiaire.) Veuillez noter que vous ne pouvez pas mettre à niveau FXOS vers une version qui ne prend pas en charge votre version de périphérique logique actuelle. Vous devrez effectuer la mise à niveau en étapes : mettez à niveau FXOS vers la version la plus élevée qui prend en charge votre périphérique logique actuel; mettez à niveau votre périphérique logique vers la version la plus élevée prise en charge avec cette version de FXOS. Par exemple, si vous souhaitez effectuer une mise à niveau de FXOS 2.2/ASA 9.8 vers FXOS 2.13/ASA 9.19, vous devrez effectuer les mises à niveau suivantes :

1. FXOS 2.2 → FXOS 2.11 (la version la plus élevée qui prend en charge la version 9.8)
2. ASA 9.8 → ASA 9.17 (la version la plus élevée prise en charge par la version 2.11)
3. FXOS 2.11 → FXOS 2.13
4. ASA 9.17 → ASA 9.19

- Défense contre les menaces : des mises à niveau provisoires peuvent être nécessaires pour défense contre les menaces , en plus des exigences FXOS ci-dessus. Pour le chemin de mise à niveau exact, consultez le centre de gestion guide de mise à niveau de votre version.
- ASA : ASA vous permet de procéder à une mise à niveau directement de votre version actuelle vers toute version supérieure, en notant les exigences FXOS ci-dessus.

Remarque FXOS 2.8(1.125) et les versions ultérieures ne prennent pas en charge ASA 9.14(1) ou 9.14(1.10) pour les sondages et les interruptions SNMP ASA; vous devez utiliser 9.14(1.15) ou une version ultérieure. Les autres versions, comme la version 9.13 ou 9.12, ne sont pas concernées.

Tableau 7 : Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.16	Firepower 4112	**9.22 (recommandé)** 9.20 9.19 9,18 9.17	**7.6** (recommandé) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115	**9.22 (recommandé)** 9.20 9.19 9,18 9.17	**7.6** (recommandé) 7.4 7.3 7.2 7.1
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.14(1)	Firepower 4112	**9.20** (recommandé) 9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.20** (recommandé) 9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.13	Firepower 4112	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.12	Firepower 4112	**9.18** (recommandé) 9.17 9.16 9.14	**7.2** (recommandé) 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2,11	Firepower 4112	**9.17** (recommandé) 9.16 9.14	**7.1** (recommandé) 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17** (recommandé) 9.16 9.14 9.12	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17** (recommandé) 9.16 9.14 9.12 9.8	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.10 **Remarque** Pour la compatibilité avec la version 7.0.2 et 9.16 (3.11) ou toute version ultérieure, vous avez besoin de FXOS 2.10 (1.179) ou une version ultérieure.	Firepower 4112	**9.16** (recommandé) 9.14	**7.0** (recommandé) 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16** (recommandé) 9.14 9.12	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16** (recommandé) 9.14 9.12 9.8	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2,8	Firepower 4112	**9.14**	**6.6** **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure.
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14** (recommandé) 9.12 **Remarque** Le Firepower 9300 SM-56 nécessite un ASA 9.12(2) ou une version ultérieure	**6.6** (recommandé) **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure. 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14** (recommandé) 9.12 9.8	**6.6** (recommandé) **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure. 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.6(1.157) **Remarque** Vous pouvez désormais exécuter un ASA 9.12 et FTD 6.4 ou toute version ultérieure sur des modules distincts du même châssis Firepower 9300	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** **Remarque** Le Firepower 9300 SM-56 nécessite un ASA 9.12.2 ou une version ultérieure	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	**6.4** (recommandé) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	Aucune prise en charge
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** La version 9.8(2.12) ou une version ultérieure est requise pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130) ou une version ultérieure.	**6.2.3** (recommandé) **Remarque** 6.2.3.16+ nécessite FXOS 2.3.1.157 ou ultérieure.
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** La version 9.8(2.12) ou une version ultérieure est requise pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130) ou une version ultérieure.	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Les versions de Défense contre les menaces sont en fin de vie
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Compatibilité avec Radware DefensePro

Le tableau suivant répertorie les versions de Radware DefensePro prises en charge pour chaque appareil de sécurité et chaque périphérique logique associé.

Tableau 8 : Compatibilité avec Radware DefensePro

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.16	9.22(1)	7.6	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145
2.14(1)	9.20(1)	7.4(1)	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.13.0	9.19(1)	7.3	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145
2.12.0	9.18(1)	7.2	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.11.1	9.17(1)	7.1	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.9.1	9.15(1)	6.7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.8.1	9.14(1)	6.6.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.7(1)	9.13(1)	6.5	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.6(1)	9.12(1) 9.10(1)	6.4.0 6.3.0	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.4(1)	9.9(2) 9.10(1)	6.2.3 6.3	8.13.01.09-2	Firepower 9300 Firepower 4110 Firepower 4120 Firepower 4140 Firepower 4150

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.3(1)	9.9(1) 9.9(2)	6.2.2 6.2.3	8.13.01.09-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense seulement) Firepower 4120 Firepower 4140 Firepower 4150
2.2(2)	9.8(1) 9.8(2) 9.8(3)	6.2.0 6.2.2	8.10.01.17-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense seulement) Firepower 4120 Firepower 4140 Firepower 4150
2.2(1)	9.7(1) 9.8(1)	6.2.0	8.10.01.17-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense seulement) Firepower 4120 Firepower 4140 Firepower 4150
2.1(1)	9.6(2) 9.6(3) 9.6(4) 9.7(1)	Aucune prise en charge	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
2.0(1)	9.6(1) 9.6(2) 9.6(3) 9.6(4)	Aucune prise en charge	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
1.1(4)	9.6(1)	Aucune prise en charge	1.1(2.32-3)	9300

Chemin de mise à niveau

Pour chaque système d'exploitation que vous mettez à niveau, vérifiez le chemin de mise à niveau pris en charge. Dans certains cas, vous devrez peut-être installer des mises à niveau intermédiaires avant de pouvoir passer à la version finale.

Chemin de mise à niveau : Appareils ASA

Pour afficher la version et le modèle actuels, utilisez l'une des méthodes suivantes :

- ASDM : Choisissez **Home** > **Device Dashboard** > **Device Information (Accueil > Tableau de bord des appareils > Informations sur les appareils)**.
- Interface de ligne de commande : Utilisez la commande **show version** .

Ce tableau fournit des chemin sde mise à niveau pour l'ASA. Certaines versions plus anciennes nécessitent une mise à niveau intermédiaire avant de pouvoir passer à une version plus récente. Les versions recommandées sont en **gras**.

Veillez à vérifier les instructions de mise à niveau pour chaque version entre votre version de départ et votre version d'arrivée. Dans certains cas, vous devrez modifier votre configuration avant de procéder à la mise à niveau, faute de quoi vous risquez de subir une panne. Voir Lignes directrices pour la mise à niveau de l'ASA, à la page 1.

Pour obtenir des informations sur les problèmes de sécurité de l'ASA et savoir quelles versions contiennent des correctifs pour chaque problème, consultez les ASA Security Advisories (avis de sécurité de l'ASA).

Remarque

ASA 9.20(x) était la version finale pour le Firepower 2100.

ASA 9.18 était la version finale pour les Firepower 4110, 4120, 4140 et 4150, et les modules de sécurité SM-24, SM-36 et SM-44 pour le Firepower 9300.

ASA 9.16 était la version finale pour les ASA 5506-X, 5508-X et 5516-X.

ASA 9.14 était la version finale pour les ASA 5525-X, 5545-X et 5555-X.

ASA 9.12 était la version finale pour les ASA 5512-X, 5515-X, 5585-X et ASASM.

ASA 9.2 était la version finale pour l'ASA 5505.

ASA 9.1(x) était la version finale pour les ASA 5510, 5520, 5540, 5550 et 5580.

Tableau 9 : Chemin de mise à niveau

Version actuelle	Version de mise à jour provisoire	Version cible
9.20	—	L'un des éléments suivants : → **9.22**

Version actuelle	Version de mise à jour provisoire	Version cible
9.19	—	L'un des éléments suivants : → **9.22** → **9.20**
9,18	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19**
9.17	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18**
9.16	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17
9.15	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**

Version actuelle	Version de mise à jour provisoire	Version cible
9.13	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14
9.12	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14
9.10	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12

Version actuelle	Version de mise à jour provisoire	Version cible
9.9	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12
9.8	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12
9.7	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8

Version actuelle	Version de mise à jour provisoire	Version cible
9.6	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.5	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.4	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8

Version actuelle	Version de mise à jour provisoire	Version cible
9.3	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.2	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), ou 9.1(7.4)	—	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.1(7.4)
9.1(1)	→ 9.1(2)	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.1(7.4)

Version actuelle	Version de mise à jour provisoire	Version cible
9.0(2), 9.0(3) ou 9.0(4)	—	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.6 → 9.1(7.4)
9.0(1)	→ 9.0(4)	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.6(1)	→ 9.0(4)	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.5(1)	→ 9.0(4)	L'un des éléments suivants : → **9.12** → 9.8 → 9.1(7.4)
8.4(5+)	—	L'un des éléments suivants : → **9.12** → 9.8 → 9.1(7.4) → 9.0(4)
8.4(1) à 8.4(4)	→ 9.0(4)	→ **9.12** → 9.8 → 9.1(7.4)
8.3	→ 9.0(4)	L'un des éléments suivants : → **9.12** → 9.8 → 9.1(7.4)

Version actuelle	Version de mise à jour provisoire	Version cible
8.2 ou version antérieure	→ 9.0(4)	L'un des éléments suivants : → **9.12** → 9.8 → 9.1(7.4)

Chemin de mise à niveau : ASA sur Firepower 2100 en mode plateforme

Pour afficher la version et le modèle actuels, utilisez l'une des méthodes suivantes :

- ASDM : Choisissez **Home** > **Device Dashboard** > **Device Information (Accueil > Tableau de bord des appareils > Informations sur les appareils)**.
- Interface de ligne de commande : Utilisez la commande **show version** .

Ce tableau fournit des chemins de mise à niveau pour l'ASA sur le Firepower 2100 en mode plateforme. Certaines versions nécessitent une mise à niveau intermédiaire avant de pouvoir passer à une version plus récente. Les versions recommandées sont en **gras**.

Veillez à vérifier les instructions de mise à niveau pour chaque version entre votre version de départ et votre version d'arrivée. Dans certains cas, vous devrez modifier votre configuration avant de procéder à la mise à niveau, faute de quoi vous risquez de subir une panne. Voir Lignes directrices pour la mise à niveau de l'ASA, à la page 1.

Pour obtenir des informations sur les problèmes de sécurité de l'ASA et savoir quelles versions contiennent des correctifs pour chaque problème, consultez les ASA Security Advisories (avis de sécurité de l'ASA).

Remarque ASA 9.20(x) était la version finale pour le Firepower 2100.

Tableau 10 : Chemin de mise à niveau

Version actuelle	Version de mise à jour provisoire	Version cible
9.19	—	L'un des éléments suivants : → **9.20**
9,18	—	L'un des éléments suivants : → **9.20** → **9.19**
9.17	—	L'un des éléments suivants : → **9.20** → **9.19** → **9.18**

Version actuelle	Version de mise à jour provisoire	Version cible
9.16	—	L'un des éléments suivants : → **9.20** → **9.19** → **9.18** → 9.17
9.15	—	L'un des éléments suivants : → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	L'un des éléments suivants : → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15
9.13	→ 9.18	L'un des éléments suivants : → **9.20** → **9.19**
9.13	—	L'un des éléments suivants : → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.12	→ 9.18	L'un des éléments suivants : → **9.20** → **9.19**

Version actuelle	Version de mise à jour provisoire	Version cible
9.12	—	L'un des éléments suivants : → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.10	→ 9.17	L'un des éléments suivants : → **9.20** → **9.19** → **9.18**
9.10	—	L'un des éléments suivants : → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.9	→ 9.17	L'un des éléments suivants : → **9.20** → **9.19** → **9.18**
9.9	—	L'un des éléments suivants : → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.8	→ 9.17	L'un des éléments suivants : → **9.20** → **9.19** → **9.18**

Version actuelle	Version de mise à jour provisoire	Version cible
9.8	—	L'un des éléments suivants : → 9.17 → **9.16** → 9.15 → 9.14 → 9.12

Chemin de mise à niveau : périphériques logiques ASA pour le Firepower 4100/9300

Pour afficher la version et le modèle actuels, utilisez l'une des méthodes suivantes :

- Firepower Chassis Manager : choisissez **Aperçu**et examinez les champs **Modèle** et **Version** dans la partie supérieure de l'écran.
- Interface de ligne de commande : pour la version, utilisez la commande **show version** et consultez le champ Paquet-Vers:. Pour le modèle, saisissez **scope chassis 1**, puis **show inventory**.
- FXOS : À partir de FXOS 2.2.2 et les versions ultérieures, vous pouvez effectuer une mise à niveau directement vers n'importe quelle version ultérieure. (FXOS 2.0.1–2.2.1 peut être mis à niveau jusqu'à la version 2.8.1. Pour les versions antérieures à la version 2.0.1, vous devez effectuer une mise à niveau à chaque version intermédiaire.) Veuillez noter que vous ne pouvez pas mettre à niveau FXOS vers une version qui ne prend pas en charge votre version de périphérique logique actuelle. Vous devrez effectuer la mise à niveau en étapes : mettez à niveau FXOS vers la version la plus élevée qui prend en charge votre périphérique logique actuel; mettez à niveau votre périphérique logique vers la version la plus élevée prise en charge avec cette version de FXOS. Par exemple, si vous souhaitez effectuer une mise à niveau de FXOS 2.2/ASA 9.8 vers FXOS 2.13/ASA 9.19, vous devrez effectuer les mises à niveau suivantes :
  1. FXOS 2.2 → FXOS 2.11 (la version la plus élevée qui prend en charge la version 9.8)
  2. ASA 9.8 → ASA 9.17 (la version la plus élevée prise en charge par la version 2.11)
  3. FXOS 2.11 → FXOS 2.13
  4. ASA 9.17 → ASA 9.19
- Défense contre les menaces : des mises à niveau provisoires peuvent être nécessaires pour défense contre les menaces , en plus des exigences FXOS ci-dessus. Pour le chemin de mise à niveau exact, consultez le centre de gestion guide de mise à niveau de votre version.
- ASA : ASA vous permet de procéder à une mise à niveau directement de votre version actuelle vers toute version supérieure, en notant les exigences FXOS ci-dessus.

Tableau 11 : Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.16	Firepower 4112	**9.22 (recommandé)** 9.20 9.19 9,18 9.17	**7.6** (recommandé) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.22 (recommandé)** 9.20 9.19 9,18 9.17	**7.6** (recommandé) 7.4 7.3 7.2 7.1
2.14(1)	Firepower 4112	**9.20** (recommandé) 9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.20** (recommandé) 9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.13	Firepower 4112	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.12	Firepower 4112	**9.18** (recommandé) 9.17 9.16 9.14	**7.2** (recommandé) 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2,11	Firepower 4112	**9.17** (recommandé) 9.16 9.14	**7.1** (recommandé) 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17** (recommandé) 9.16 9.14 9.12	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17** (recommandé) 9.16 9.14 9.12 9.8	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.10 **Remarque** Pour la compatibilité avec la version 7.0.2 et 9.16 (3.11) ou toute version ultérieure, vous avez besoin de FXOS 2.10 (1.179) ou une version ultérieure.	Firepower 4112	**9.16** (recommandé) 9.14	**7.0** (recommandé) 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16** (recommandé) 9.14 9.12	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16** (recommandé) 9.14 9.12 9.8	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2,8	Firepower 4112	**9.14**	**6.6** **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure.
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14** (recommandé) 9.12 **Remarque** Le Firepower 9300 SM-56 nécessite un ASA 9.12(2) ou une version ultérieure	**6.6** (recommandé) **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure. 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14** (recommandé) 9.12 9.8	**6.6** (recommandé) **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure. 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.6(1.157) **Remarque** Vous pouvez désormais exécuter un ASA 9.12 et FTD 6.4 ou toute version ultérieure sur des modules distincts du même châssis Firepower 9300	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** **Remarque** Le Firepower 9300 SM-56 nécessite un ASA 9.12.2 ou une version ultérieure	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	**6.4** (recommandé) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	Aucune prise en charge
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** La version 9.8(2.12) ou une version ultérieure est requise pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130) ou une version ultérieure.	**6.2.3** (recommandé) **Remarque** 6.2.3.16+ nécessite FXOS 2.3.1.157 ou ultérieure.
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** La version 9.8(2.12) ou une version ultérieure est requise pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130) ou une version ultérieure.	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Les versions de Défense contre les menaces sont en fin de vie
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Remarque sur les rétrogradations

La rétrogradation des images FXOS n'est pas officiellement prise en charge. La seule méthode prise en charge par Cisco pour rétrograder une version d'image FXOS consiste à effectuer une recréation d'image complète de l'appareil.

Télécharger le logiciel à partir de Cisco.com

Téléchargez tous les paquets de logiciels à partir de Cisco.com avant de commencer la mise à niveau. Selon le système d'exploitation et si vous utilisez l'interface de ligne de commande ou l'interface graphique, vous devez placer les images sur un serveur ou sur votre ordinateur de gestion. Consultez chaque procédure d'installation pour connaître les détails sur les emplacements de fichiers pris en charge.

Remarque Un identifiant Cisco.com et un contrat de service Cisco sont requis.

Télécharger le logiciel ASA

Si vous utilisez l'assistant de mise à niveau ASDM, vous n'avez pas besoin de prétélécharger le logiciel. Si vous effectuez une mise à niveau manuelle, par exemple pour une mise à niveau de basculement, téléchargez les images sur votre ordinateur local.

Pour procéder à une mise à niveau de l'interface de ligne de commande, vous pouvez placer le logiciel sur de nombreux types de serveurs, notamment TFTP, HTTP et FTP. Consultez les commandes **copy** dans la référence de commande ASA.

Le logiciel ASA peut être téléchargé à partir du site Cisco.com. Ces tableaux comprennent des conventions de dénomination et des informations sur les paquets ASA.

Tableau 12 : Plateformes actuelles

Modèle ASA	Emplacement de téléchargement	Progiciels
ASA virtuel	http://www.cisco.com/go/asav-software	
	Logiciel ASA (mise à niveau) Choisissez **Logiciel d'appareils de sécurité adaptables (ASA)** > *version*.	Le fichier de mise à niveau virtuelle ASA porte un nom de fichier de type asa962-**smp-k8.bin**; utilisez ce fichier de mise à niveau pour tous les hyperviseurs. **Remarque :** Les fichiers .zip (VMware), .vhdx (Hyper-V) et .qcow2 (KVM) sont réservés au déploiement initial. **Remarque** Pour mettre à niveau l'ASA virtuel pour les services en nuage public tels que Amazon Web Services, vous pouvez télécharger l'image ci-dessus à partir de Cisco.com (qui nécessite un identifiant Cisco.com et un contrat de service Cisco) et effectuer la mise à niveau comme décrit dans ce guide. Il n'y a aucun moyen d'obtenir une image de *mise à niveau* à partir du service de nuage public.
	Logiciel ASDM (mise à niveau) Choisissez **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.
	Paquet de périphérique ASA pour APIC (Cisco Application Policy Infrastructure Controller) Choisissez **Paquets de périphériques ASA pour l'infrastructure axée sur les applications (ACI)** > *version*.	Pour APIC 1.2(7) et les versions ultérieures, choisissez le paquet Policy Orchestration avec Fabric Insertion ou le paquet Fabric Insertion seul. Exemple de nom de fichier utilisé pour le paquet de périphérique : asa-device-pkg-1.2.7.10**.zip**. Pour installer le paquet de périphérique ASA, consultez le chapitre « Importation d'un paquet de périphérique » du Guide de déploiement des services APIC de Cisco pour les couches 4 à 7.

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower 1000	http://www.cisco.com/go/asa-firepower-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-fp1k.9.13.1**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7131**.bin**. **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-7131.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.

Modèle ASA	Emplacement de téléchargement	Progiciels
Secure Firewall 1200	http://www.cisco.com/go/asa-firepower-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-csf1200.9.22.1.3**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7221**.bin**. **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-7221.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.

Modèle ASA	Emplacement de téléchargement	Progiciels
Secure Firewall 3100	https://cisco.com/go/asa-secure-firewall-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-fp3k.9.17.1**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7171**.bin**. **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-7171.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.

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower 4100	http://www.cisco.com/go/firepower4100-software	
	Logiciels ASA et ASDM Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Ce paquet comprend ASA et ASDM. Exemple de nom de fichier pour le paquet ASA : cisco-ASA.9.6.2**.SPA.csp**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**. **Remarque** Lorsque vous mettez à niveau le paquet de l'ASA dans FXOS, 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.
	Logiciel API REST Choisissez votre *modèle* > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.

Modèle ASA	Emplacement de téléchargement	Progiciels
Secure Firewall 4200	https://cisco.com/go/asa-secure-firewall-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-fp4200.9.20.1**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7201**.bin**. **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-7201.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.

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower 9300	http://www.cisco.com/go/firepower9300-software	
	Logiciels ASA et ASDM Choisissez **Logiciel d'appareils de sécurité adaptables (ASA)** > *version*.	Ce paquet comprend ASA et ASDM. Exemple de nom de fichier pour le paquet ASA : cisco-ASA.9.6.2**.SPA.csp**.
	Logiciel ASDM (mise à niveau) Choisissez **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**. **Remarque** Lorsque vous mettez à niveau le paquet de l'ASA dans FXOS, 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.
	Logiciel API REST Choisissez **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.

Modèle ASA	Emplacement de téléchargement	Progiciels
ISA 3000	http://www.cisco.com/go/isa3000-software	
	Logiciel ASA Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**lfbff-k8.SPA**.
	Logiciel ASDM Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.

Tableau 13 : Plateformes existantes

Modèle ASA	Emplacement de téléchargement	Progiciels
ASA 5506-X, ASA 5508-X et ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	Logiciel ASA Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**lfbff-k8.SPA**.
	Logiciel ASDM Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.
	Logiciel ROMMON Choisissez votre *modèle* > **Logiciel Rommon pour ASA** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ROMMON : asa5500-firmware-1108**.SPA**.

Modèle ASA	Emplacement de téléchargement	Progiciels
ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X et ASA 5555-X	http://www.cisco.com/go/asa-software	
	Logiciel ASA Choisissez votre *modèle* > **Logiciels sur châssis** > **Logiciel d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**smp-k8.bin**.
	Logiciel ASDM Choisissez votre *modèle* > **Logiciels sur châssis** > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Logiciels sur châssis** > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.
	Paquet de périphérique ASA pour APIC (Cisco Application Policy Infrastructure Controller) Choisissez votre *modèle* > **Logiciels sur châssis** > **Paquets de périphériques ASA pour l'infrastructure axée sur les applications (ACI)** > *version*.	Pour APIC 1.2(7) et les versions ultérieures, choisissez le paquet Policy Orchestration avec Fabric Insertion ou le paquet Fabric Insertion seul. Exemple de nom de fichier utilisé pour le paquet de périphérique : asa-device-pkg-1.2.7.10**.zip**. Pour installer le paquet de périphérique ASA, consultez le chapitre « Importation d'un paquet de périphérique » du Guide de déploiement des services APIC de Cisco pour les couches 4 à 7.

Modèle ASA	Emplacement de téléchargement	Progiciels
ASA 5585-X	http://www.cisco.com/go/asa-software	
	Logiciel ASA Choisissez votre *modèle* > **Logiciels sur châssis** > **Logiciel d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**smp-k8.bin**.
	Logiciel ASDM Choisissez votre *modèle* > **Logiciels sur châssis** > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Logiciels sur châssis** > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.
	Paquet de périphérique ASA pour APIC (Cisco Application Policy Infrastructure Controller) Choisissez votre *modèle* > **Logiciels sur châssis** > **Paquets de périphériques ASA pour l'infrastructure axée sur les applications (ACI)** > *version*.	Pour APIC 1.2(7) et les versions ultérieures, choisissez le paquet Policy Orchestration avec Fabric Insertion ou le paquet Fabric Insertion seul. Exemple de nom de fichier utilisé pour le paquet de périphérique : asa-device-pkg-1.2.7.10**.zip**. Pour installer le paquet de périphérique ASA, consultez le chapitre « Importation d'un paquet de périphérique » du Guide de déploiement des services APIC de Cisco pour les couches 4 à 7.

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower de la série 2100	http://www.cisco.com/go/asa-firepower-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-fp2k.9.8.2**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-782**.bin**. **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.
ISA 3000	http://www.cisco.com/go/isa3000-software	
	Logiciel ASA Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**lfbff-k8.SPA**.
	Logiciel ASDM Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.

Télécharger FXOS pour le Firepower 4100/9300

Les paquets FXOS pour les périphériques Firepower 4100/9300 sont disponibles sur le Site d'assistance et de téléchargement Cisco.

- Firepower 4100 : http://www.cisco.com/go/firepower4100-software
- Firepower 9300 : http://www.cisco.com/go/firepower9300-software

Pour trouver des progiciels FXOS, sélectionnez ou recherchez votre modèle d'appareil Firepower, puis accédez à la page de téléchargement de Firepower Extensible Operating System pour obtenir la version cible.

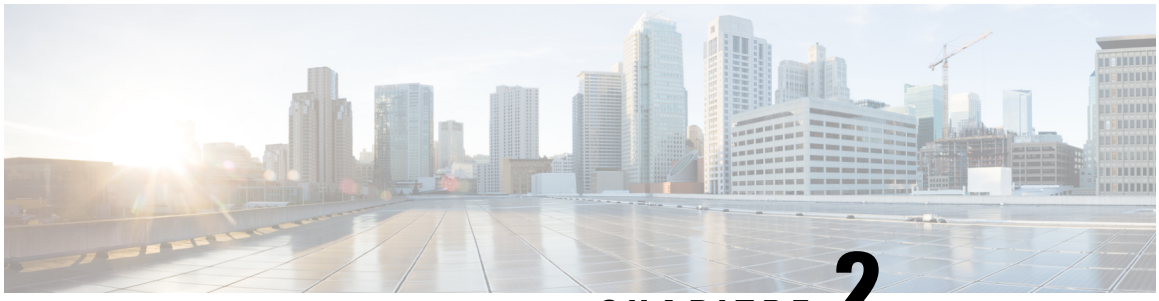
Remarque Si vous prévoyez d'utiliser l'interface de ligne de commande pour mettre à niveau FXOS, copiez le paquet de mise à niveau sur un serveur auquel Firepower 4100/9300 peut accéder en utilisant le protocole SCP, SFTP, TFTP ou FTP.

Tableau 14 : Paquets FXOS pour Firepower 4100/9300

Type de package	Ensemble
Image FXOS	fxos-k9.*version*.**SPA**
Récupération (démarrage)	fxos-k9-**kickstart**.*version*.**SPA**
Récupération (gestionnaire)	fxos-k9-**manager**.*version*.**SPA**
Récupération (système)	fxos-k9-**system**.*version*.**SPA**
Bases d'informations de gestion (MIB)	fxos-**mibs**-fp9k-fp4k.*version*.**zip**
Micrologiciel : Firepower 4100	fxos-k9-fpr4k-**firmware**.*version*.**SPA**
Micrologiciel : Firepower 9300	fxos-k9-fpr9k-**firmware**.*version*.**SPA**

Sauvegarder vos configurations

Nous vous recommandons de sauvegarder vos configurations et autres fichiers critiques avant d'effectuer la mise à niveau, en particulier s'il y a migration de configuration. Chaque système d'exploitation utilise une méthode différente pour effectuer les sauvegardes. Pour en savoir plus, consultez les guides de configuration d'ASA, d'ASDM, de gestion locale ASA FirePOWER, de Firepower Management Center et de FXOS.



CHAPITRE 2

Mettre à niveau l'ASA

Mettez à niveau l'ASA en fonction des procédures du présent document.

- Mettre à niveau l'appareil ASA, à la page 75
- Mettre à niveau le Firepower 4100/9300, à la page 94
- Mettre à niveau l'ASA Virtual, l'ISA 3000 ou l'ASA 5500-X, à la page 129
- Mettre à niveau le Firepower 2100 en mode plateforme, à la page 153

Mettre à niveau l'appareil ASA

Ce document décrit comment planifier et mettre en œuvre une mise à niveau ASA, FXOS et ASDM pour les déploiements autonomes, de basculement ou de mise en grappe sur les modèles suivants :

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

Pour le Firepower 2100 en version 9.12 et toute version antérieure, seul le mode plateforme est disponible. Dans les versions 9.13 et ultérieures, le mode appareil est le mode par défaut. Vérifiez le mode à l'aide de la commande **show fxos mode** sur l'interface de ligne de commande de l'ASA.

Mettre à niveau une unité autonome

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau l'unité autonome.

Mettre à niveau une unité autonome à l'aide de l'interface de ligne de commande

Cette section décrit comment installer les images ASDM et ASA sur le Firepower 1000, le Firepower 2100 en mode appareil et le Secure Firewall 3100/4200.

Avant de commencer

Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Procédure

Étape 1 En mode de configuration globale, si vous avez précédemment défini une image ASDM autre que celle par défaut, réinitialisez-la à l'image fournie avec votre ensemble d'images.

asdm image disk0:/asdm.bin

write memory

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

Étape 2 En mode d'exécution privilégié (minimum), copiez le logiciel ASA dans la mémoire flash.

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa*
disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Étape 3 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Étape 4 Affiche l'image de démarrage actuelle configurée, si elle est présente.

show running-config boot system

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.

Exemple :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Étape 5 Si vous avez configuré une commande **boot system**, supprimez-la pour pouvoir saisir la nouvelle image de démarrage.

no boot system disk*n*:/[*chemin*/]*nom_de_l_image_asa*

Si aucune commande **boot system** n'est configurée, ignorez cette étape.

Exemple :

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Étape 6 Définissez l'image ASA à démarrer (celle que vous venez de charger).

boot system disk*n*:/[*chemin*/]*nom_de_l_image_asa*

Vous ne pouvez saisir qu'une seule commande **boot system**. 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 procéder au rechargement, 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.

Exemple :

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.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 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
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
ciscoasa(config)#
```

Étape 7 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Étape 8 Rechargez l'ASA :

reload

Mettre à niveau une unité autonome à partir de votre ordinateur local à l'aide d'ASDM

L'**outil de mise à niveau du logiciel à partir de l'ordinateur local** vous permet de charger un fichier image de votre ordinateur vers le système de fichiers flash pour mettre à niveau l'ASA pour le Firepower 1000, le Firepower 2100 en mode appareil et le Secure Firewall 3100/4200.

Procédure

Étape 1 Si vous avez précédemment défini une image ASDM autre que celle par défaut, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Dans la fenêtre principale de l'application ASDM, choisissez **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** (Configuration, Gestion de appareils, Image/Configuration du système, Image/Configuration de démarrage).
b) Pour le **chemin d'accès au fichier image ASDM**, saisissez **disk0:/asdm.bin**.
c) Cliquez sur **Apply**.

Étape 2 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

Étape 3 Dans la liste déroulante **Image à charger**, sélectionnez **ASA**.

Étape 4 Dans le champ **Chemin d'accès au fichier local**, cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 5 Dans le champ **Chemin d'accès au système de fichiers flash**, cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Étape 6 Cliquez sur **Charger une image**.

Le processus de chargement peut prendre quelques minutes.

Étape 7 Vous êtes invité à définir cette image comme image ASA. Cliquez sur **Yes** (Oui).

Étape 8 Il vous est rappelé de recharger l'ASA pour utiliser la nouvelle image. Cliquez sur **OK**.

Vous quittez l'outil **Mise à niveau**.

Étape 9 Choisissez **Outils** > **Rechargement du système** pour recharger l'ASA.

Une nouvelle fenêtre s'affiche et vous demande de vérifier les détails du rechargement.

a) Cliquez sur le bouton radio **Enregistrer la configuration en cours d'enregistrement au moment du rechargement**.
b) Choisissez une heure de rechargement (par exemple, **Maintenant**, la valeur par défaut).
c) Cliquer sur **Planifier le rechargement**.

Une fois que le rechargement est en cours, une fenêtre **État du rechargement** s'affiche pour indiquer qu'un rechargement est en cours. Une option pour quitter ASDM est également fournie.

Étape 10 Après le rechargement de l'ASA, redémarrez ASDM.

Vous pouvez vérifier l'état de rechargement à partir d'un port de console, ou vous pouvez attendre quelques minutes et essayer de vous connecter à l'aide d'ASDM.

Mettre à niveau une unité autonome à l'aide de l'assistant ASDM Cisco.com

L'**assistant de mise à niveau du logiciel à partir de Cisco.com** vous permet de mettre à niveau automatiquement ASDM et ASA vers des versions plus récentes pour le Firepower 1000, le Firepower 2100 en mode appareil et le Secure Firewall 3100.

Dans cet assistant, vous pouvez effectuer les opérations suivantes :

- Choisissez un fichier image ASA ou un fichier image ASDM à mettre à niveau.

Remarque ASDM télécharge la dernière version de l'image, qui comprend le numéro de version. Par exemple, si vous téléchargez la version 9.9(1), le téléchargement peut inclure la version 9.9(1.2). Ce comportement est normal, vous pouvez donc procéder à la mise à niveau prévue.

- Passez en revue les modifications de mise à niveau que vous avez apportées.
- Téléchargez l'image ou les images et installez-les.
- Passez en revue l'état de l'installation.
- Si l'installation a réussi, rechargez l'ASA pour enregistrer la configuration et terminer la mise à niveau.

Avant de commencer

En raison d'une modification interne, l'assistant est uniquement pris en charge par ASDM 7.10(1) ou les versions ultérieures. De plus, en raison d'une modification de nom d'image, vous devez utiliser ASDM 7.12(1) ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.10(1) ou une version ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM, quelle que soit la version d'ASA que vous utilisez.

Procédure

Étape 1 Choisissez **Outils** > **Vérifier la présence de mises à jour ASA/ASDM**.

En mode contexte multiple, accédez à ce menu à partir du système.

La boîte de dialogue **Authentification de Cisco.com** s'affiche.

Étape 2 Saisissez votre nom d'utilisateur et votre mot de passe Cisco.com, puis cliquez sur **Connexion**.

L'**assistant de mise à niveau Cisco.com** s'affiche.

Remarque
Si aucune mise à niveau n'est disponible, une boîte de dialogue s'affiche. Cliquez sur **OK** pour quitter l'assistant.

Étape 3 Cliquez sur **Suivant** pour afficher l'écran **Sélectionner un logiciel**.

La version d'ASA actuelle et la version d'ASDM s'affichent.

Étape 4 Pour mettre à niveau la version d'ASA et la version d'ASDM, procédez comme suit :

a) Dans la zone **ASA**, cochez la case **Mettre à niveau vers**, puis choisissez une version d'ASA à laquelle vous souhaitez passer dans la liste déroulante.
b) Dans la zone **ASDM**, cochez la case **Mettre à niveau vers**, puis choisissez une version d'ASDM à laquelle vous souhaitez passer dans la liste déroulante.

Étape 5 Cliquez sur **Suivant** pour afficher l'écran **Passer en revue les modifications**.

Étape 6 Vérifiez les éléments suivants :

- Le fichier image ASA ou le fichier image ASDM que vous avez téléchargé est le bon.
- Le fichier image ASA ou le fichier image ASDM que vous souhaitez charger est le bon.
- La bonne image de démarrage ASA a été sélectionnée.

Étape 7 Cliquez sur **Suivant** pour lancer l'installation de la mise à niveau.

Vous pouvez ensuite afficher l'état de l'installation de la mise à niveau à mesure qu'elle progresse.

L'écran **Résultats** s'affiche, et fournit des détails supplémentaires, comme l'état de l'installation de la mise à niveau (réussite ou échec).

Étape 8 Si l'installation de la mise à niveau a réussi, pour que les versions de mise à niveau prennent effet, cochez la case **Enregistrer la configuration et recharger le périphérique maintenant** pour redémarrer l'ASA et le redémarrer ASDM.

Étape 9 Cliquez sur **Terminer** pour quitter l'assistant et enregistrer les modifications de configuration que vous avez apportées.

Remarque
Pour passer à la version ultérieure, le cas échéant, vous devez redémarrer l'assistant.

Étape 10 Après le rechargement de l'ASA, redémarrez ASDM.

Vous pouvez vérifier l'état de rechargement à partir d'un port de console, ou vous pouvez attendre quelques minutes et essayer de vous connecter à l'aide d'ASDM.

Mettre à niveau une paire de basculements actif/de secours

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau la paire de basculements actif/de secours pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une paire de basculements actif/de secours à l'aide de l'interface de ligne de commande

Pour mettre à niveau la paire de basculements actif/de secours pour le Firepower 1000, le Firepower 2100 en mode appareil et le Secure Firewall 3100/4200, procédez comme suit.

Avant de commencer

- Exécutez ces étapes sur l'unité active. Pour l'accès SSH, connectez-vous à l'adresse IP active; l'unité active présente toujours cette adresse IP. Lorsque vous vous connectez à l'interface de ligne de commande, déterminez l'état de basculement en examinant l'invite d'ASA; vous pouvez configurer l'invite ASA pour afficher l'état et la priorité de basculement (principal ou secondaire), ce qui est utile pour déterminer

à quelle unité vous êtes connecté. Consultez la commande d'invite. Vous pouvez également saisir la commande **show failover** pour afficher l'état et la priorité de cette unité (principale ou secondaire).

- Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Procédure

Étape 1 Sur l'unité principale en mode de configuration globale, si vous avez précédemment défini une image ASDM autre que celle par défaut, réinitialisez-la à l'image fournie avec votre ensemble d'images.

asdm image disk0:/asdm.bin

write memory

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

Étape 2 Sur l'unité active, en mode d'exécution privilégié (minimum), copiez le logiciel ASA dans la mémoire flash de l'unité active :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa*
disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Étape 3 Copiez le logiciel sur l'unité de secours. Assurez-vous de définir le même chemin que pour l'unité active :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Étape 4 Si vous n'êtes pas déjà en mode de configuration globale, accédez-y :

configure terminal

Étape 5 Affiche l'image de démarrage actuelle configurée, si elle est présente.

show running-config boot system

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.

Exemple :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Étape 6 Si vous avez configuré une commande **boot system**, supprimez-la pour pouvoir saisir la nouvelle image de démarrage.

no boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Si aucune commande **boot system** n'est configurée, ignorez cette étape.

Exemple :

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Étape 7 Définissez l'image ASA à démarrer (celle que vous venez de charger).

boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Vous ne pouvez saisir qu'une seule commande **boot system**. 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 procéder au rechargement, 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.

Exemple :

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.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 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
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
ciscoasa(config)#
```

Étape 8 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Ces modifications de configuration sont automatiquement enregistrées sur l'unité de secours.

Étape 9 Rechargez l'unité de secours pour démarrer la nouvelle image :

failover reload-standby

Attendez que l'unité de secours ait terminé le chargement. Utilisez la commande **show failover** pour vérifier que l'unité de secours est à l'état de secours.

Étape 10 Forcez l'unité active à basculer vers l'unité de secours.

no failover active

Si vous êtes déconnecté de votre session SSH, reconnectez-vous à l'adresse IP principale, maintenant sur la nouvelle unité active/ancienne unité de secours.

Étape 11 À partir de la nouvelle unité active, rechargez l'ancienne unité active (maintenant la nouvelle unité de secours).

failover reload-standby

Exemple :

```
asa/act# failover reload-standby
```

Remarque
Si vous êtes connecté au port de console de l'ancienne unité active, vous devez plutôt saisir la commande **reload** pour recharger l'ancienne unité active.

Mettre à niveau une paire de basculements actif/de secours à l'aide d'ASDM

L'**outil de mise à niveau du logiciel à partir de l'ordinateur local** vous permet de charger un fichier image de votre ordinateur vers le système de fichiers flash pour mettre à niveau la paire de basculements actif/de secours pour le Firepower 1000, le Firepower 2100 en mode appareil et le Secure Firewall 3100/4200.

Procédure

Étape 1 Lancez ASDM sur l'unité *de secours* en vous connectant à l'adresse IP de secours.

Étape 2 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 3 Dans la liste déroulante **Image à charger**, sélectionnez **ASA**.

Étape 4 Dans le champ **Chemin d'accès au fichier local**, saisissez le chemin d'accès local au fichier sur votre ordinateur ou cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 5 Dans le champ **Chemin d'accès au système de fichiers flash**, saisissez le chemin d'accès au système de fichiers flash ou cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Étape 6 Cliquez sur **Charger une image**. Le processus de chargement peut prendre quelques minutes.

Lorsque vous êtes invité à définir cette image comme image ASA, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 7 Connectez ASDM à l'unité *active* en vous connectant à l'adresse IP principale.

Étape 8 Si vous avez précédemment défini une image ASDM autre que celle par défaut, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Choisissez **Configuration** > **Gestion des périphériques** > **Image du système/Configuration** > **Image de démarrage/Configuration**.
b) Pour le **chemin d'accès au fichier image ASDM**, saisissez **disk0:/asdm.bin**.
c) Cliquez sur **Apply**.

Étape 9 Chargez le logiciel ASA en utilisant le même emplacement de fichier que vous avez utilisé sur l'unité de secours.

Étape 10 Lorsque vous êtes invité à définir l'image comme image ASA, cliquez sur **Oui**.

Il vous est rappelé de recharger l'ASA pour utiliser la nouvelle image. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau.

Étape 11 Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Ces modifications de configuration sont automatiquement enregistrées sur l'unité de secours.

Étape 12 Rechargez l'unité de secours en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Recharger l'unité de secours**.

Restez dans le volet **Système** pour surveiller le rechargement de l'unité de secours.

Étape 13 Après le rechargement de l'unité de secours, forcez l'unité active à basculer vers l'unité de secours en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Faire passer en groupe de secours**.

ASDM se reconnectera automatiquement à la nouvelle unité active.

Étape 14 Rechargez l'unité de secours (nouvelle) en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Recharger l'unité de secours**.

Mettre à niveau une paire de basculements actif/actif

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau la paire de basculements actif/actif pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une paire de basculements actif/actif à l'aide de l'interface de ligne de commande

Pour mettre à niveau deux unités dans une configuration de basculement actif/actif, effectuez les étapes suivantes sur le Firepower 1000, le Firepower 2100 en mode appareil et le Secure Firewall 3100/4200.

Avant de commencer

- Exécutez ces étapes sur l'unité principale.
- Effectuez ces étapes dans l'espace d'exécution du système.

- Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Procédure

Étape 1 Sur l'unité principale en mode de configuration globale, si vous avez précédemment défini une image ASDM autre que celle par défaut, réinitialisez-la à l'image fournie avec votre ensemble d'images.

asdm image disk0:/asdm.bin

write memory

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

Étape 2 Sur l'unité principale, en mode d'exécution privilégié (minimum), copiez le logiciel ASA dans la mémoire flash :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa*
disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Remarque
ASDM est inclus dans l'image ASA.

Exemple :

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Étape 3 Copiez le logiciel sur l'unité secondaire. Assurez-vous de définir le même chemin que pour l'unité principale :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Étape 4 Si vous n'êtes pas déjà en mode de configuration globale, accédez-y :

configure terminal

Étape 5 Affiche l'image de démarrage actuelle configurée, si elle est présente.

show running-config boot system

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.

Exemple :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Étape 6 Si vous avez configuré une commande **boot system**, supprimez-la pour pouvoir saisir la nouvelle image de démarrage.

no boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Si aucune commande **boot system** n'est configurée, ignorez cette étape.

Exemple :

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Étape 7 Définissez l'image ASA à démarrer (celle que vous venez de charger).

boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Vous ne pouvez saisir qu'une seule commande **boot system**. 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 procéder au rechargement, 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.

Exemple :

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.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 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
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
ciscoasa(config)#
```

Étape 8 Enregistrez les nouveaux paramètres dans la configuration de démarrage.

write memory

Ces modifications de configuration sont automatiquement enregistrées sur l'unité secondaire.

Étape 9 Activez les deux groupes de basculement sur l'unité principale.

failover active group 1

failover active group 2

Exemple :

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

Étape 10 Rechargez l'unité secondaire pour démarrer la nouvelle image :

failover reload-standby

Attendez que l'unité secondaire ait terminé le chargement. Utilisez la commande **show failover** pour vérifier que les deux groupes de basculement sont à l'état de secours.

Étape 11 Forcez les deux groupes de basculement à devenir actifs sur l'unité secondaire :

no failover active group 1

no failover active group 2

Exemple :

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

Si vous êtes déconnecté de votre session SSH, reconnectez-vous à l'adresse IP du groupe de basculement 1, maintenant sur l'unité secondaire.

Étape 12 Rechargez l'unité principale :

failover reload-standby

Exemple :

```
asa/act/sec# failover reload-standby
```

Remarque
Si vous êtes connecté au port de console de l'unité principale, vous devez plutôt saisir la commande **reload** pour recharger l'unité principale.

Il se peut que vous soyez déconnecté de votre session SSH.

Étape 13 Si les groupes de basculement sont configurés avec la commande **preempt**, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé.

Mettre à niveau une paire de basculements actif/actif à l'aide d'ASDM

L'**outil de mise à niveau du logiciel à partir de l'ordinateur local** vous permet de charger un fichier image de votre ordinateur vers le système de fichiers flash pour mettre à niveau la paire de basculements actif/actif pour le Firepower 1000, le Firepower 2100 en mode appareil et le Secure Firewall 3100/4200.

Avant de commencer

- Effectuez ces étapes dans l'espace d'exécution du système.

- Placez l'image ASA sur votre ordinateur de gestion local.

Procédure

Étape 1 Lancez ASDM sur l'unité *secondaire* en vous connectant à l'adresse de gestion dans le groupe de basculement 2.

Étape 2 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 3 Dans la liste déroulante **Image à charger**, sélectionnez **ASA**.

Étape 4 Dans le champ **Chemin d'accès au fichier local**, saisissez le chemin d'accès local au fichier sur votre ordinateur ou cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 5 Dans le champ **Chemin d'accès au système de fichiers flash**, saisissez le chemin d'accès au système de fichiers flash ou cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Étape 6 Cliquez sur **Charger une image**. Le processus de chargement peut prendre quelques minutes.

Lorsque vous êtes invité à définir cette image comme image ASA, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 7 Connectez ASDM sur l'unité *principale* en vous connectant à l'adresse IP de gestion dans le groupe de basculement 1.

Étape 8 Si vous avez précédemment défini une image ASDM autre que celle par défaut, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Choisissez **Configuration** > **Gestion des périphériques** > **Image du système/Configuration** > **Image de démarrage/Configuration**.
b) Pour le **chemin d'accès au fichier image ASDM**, saisissez **disk0:/asdm.bin**.
c) Cliquez sur **Apply**.

Étape 9 Chargez le logiciel ASA en utilisant le même emplacement de fichier que vous avez utilisé sur l'unité secondaire.

Étape 10 Lorsque vous êtes invité à définir l'image comme image ASA, cliquez sur **Oui**.

Il vous est rappelé de recharger l'ASA pour utiliser la nouvelle image. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau.

Étape 11 Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Ces modifications de configuration sont automatiquement enregistrées sur l'unité secondaire.

Étape 12 Activez les deux groupes de basculement sur l'unité principale en sélectionnant **Surveillance** > **Basculement** > **Groupe de basculement #**, où **#** est le numéro du groupe de basculement que vous souhaitez déplacer dans l'unité principale, puis cliquez sur **Faire passer en groupe actif**.

Étape 13 Rechargez l'unité secondaire en sélectionnant **Surveillance** > **Basculement** > **Système**, puis cliquez sur **Recharger l'unité de secours**.

Restez dans le volet **Système** pour surveiller le rechargement de l'unité secondaire.

Étape 14 Après le déploiement de l'unité secondaire, activez les deux groupes de basculement sur l'unité secondaire en sélectionnant **Surveillance** > **Basculement** > **Groupe de basculement #**, où **#** est le numéro du groupe de basculement que vous souhaitez déplacer dans l'unité secondaire, puis cliquez sur **Faire passer en groupe de secours**.

ASDM se reconnectera automatiquement à l'adresse IP du groupe de basculement 1 sur l'unité secondaire.

Étape 15 Rechargez l'unité principale en sélectionnant **Surveillance** > **Basculement** > **Système**, puis cliquez sur **Recharger l'unité de secours**.

Étape 16 Si les groupes de basculement sont configurés avec la préemption activée, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé. ASDM se reconnectera automatiquement à l'adresse IP du groupe de basculement 1 sur l'unité principale.

Mettre à niveau une grappe ASA (Secure Firewall 3100/4200)

-

Mettre à niveau une grappe ASA à l'aide de l'interface de ligne de comande (Secure Firewall 3100/4200)

Pour mettre à niveau tous les nœuds d'une grappe ASA, suivez les étapes suivantes. Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Avant de commencer

- Exécutez ces étapes sur le nœud de contrôle. Vous pouvez configurer l'invite ASA pour afficher le nœud de la grappe et son état (contrôle ou données), ce qui est utile pour déterminer à quel nœud vous êtes connecté. Consultez la commande d'invite. Vous pouvez également saisir la commande **show cluster info** pour afficher le rôle de chaque nœud.
- Vous devez utiliser le port de console; vous ne pouvez pas activer ni désactiver la mise en grappe à partir d'une connexion distante d'interface de ligne de commande.
- Effectuez ces étapes dans l'espace d'exécution du système pour le mode contexte multiple.

Procédure

Étape 1 Sur le nœud de contrôle en mode de configuration globale, si vous avez précédemment défini une image ASDM autre que celle par défaut, réinitialisez-la à l'image fournie avec votre ensemble d'images.

asdm image disk0:/asdm.bin

write memory

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

Étape 2 Sur le nœud de contrôle en mode d'exécution privilégié (minimum), copiez le logiciel ASA sur tous les nœuds de la grappe.

cluster exec copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/unit1/control# cluster exec copy /noconfirm
ftp://dwinchester:sam@10.1.1.1/cisco-asa-fp3k.9.19.1.SPA disk0:/cisco-asa-fp3k.9.19.1.SPA
```

Étape 3 Si vous n'êtes pas déjà en mode de configuration globale, accédez-y maintenant.

configure terminal

Exemple :

```
asa/unit1/control# configure terminal
asa/unit1/control(config)#
```

Étape 4 Affiche l'image de démarrage actuelle configurée, si elle est présente.

show running-config boot system

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.

Exemple :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.17.1.SPA
```

Étape 5 Si vous avez configuré une commande **boot system**, supprimez-la pour pouvoir saisir la nouvelle image de démarrage.

no boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Si aucune commande **boot system** n'est configurée, ignorez cette étape.

Exemple :

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.17.1.SPA
```

Étape 6 Définissez l'image ASA à démarrer (celle que vous venez de charger).

boot system disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Vous ne pouvez saisir qu'une seule commande **boot system**. 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 procéder au rechargement, 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.

Exemple :

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.19.1.SPA

The system is currently installed with security software package 9.17.1, which has:
   - The platform version:  2.11.1
   - The CSP (asa) version: 9.17.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.19.1 will do the following:
   - upgrade to the new platform version 2.13.1
   - upgrade to the CSP ASA version 9.19.1
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
ciscoasa(config)#
```

Étape 7 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Ces modifications de configuration sont automatiquement enregistrées sur les nœuds de données.

Étape 8 Mettez à niveau les nœuds de données en les rechargeant.

Remarque
Pendant le processus de mise à niveau, n'utilisez jamais la commande **cluster control-node unit** pour forcer un nœud de données à devenir le nœud de contrôle; vous pouvez causer des problèmes de connectivité au réseau et de stabilité de grappe. Vous devez d'abord procéder à une mise à niveau et recharger tous les nœuds de données, puis poursuivre cette procédure pour assurer une transition harmonieuse du nœud de contrôle actuel vers un nouveau nœud de contrôle.

a) Sur le nœud de contrôle, pour afficher les noms de membre, saisissez **cluster exec unit ?**, ou saisissez la commande **show cluster info**.
b) Rechargez un nœud de données.

   cluster exec unit *data-node* **reload noconfirm**

   Exemple :

   ```
   asa/unit1/control# cluster exec unit node2 reload noconfirm
   ```

c) Répétez l'opération pour chaque nœud de données.

Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque nœud soit de nouveau opérationnel et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour le nœud suivant. Pour savoir quand un nœud rejoint la grappe, saisissez **show cluster info**.

Étape 9 Mettez à niveau le nœud de contrôle en le rechargeant.

a) Désactivez la mise en grappe. Nous vous recommandons de désactiver manuellement la mise en grappe sur le nœud de contrôle si possible afin qu'un nouveau nœud de contrôle puisse être choisi aussi rapidement et proprement que possible.

cluster group *name*

no enable

Attendez 5 minutes qu'un nouveau nœud de contrôle soit sélectionné et que le trafic se stabilise.

N'enregistrez pas cette configuration; vous voulez que la mise en grappe soit activée lorsque vous rechargez le nœud.

Exemple :

```
asa/unit1/control(config)# cluster group cluster1
asa/unit1/control(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
either enable clustering or remove cluster group configuration.

Cluster unit node1 transitioned from CONTROL to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) Rechargez ce nœud.

reload noconfirm

Lorsque l'ancien nœud de contrôle rejoint la grappe, il devient un nœud de données.

Mettre à niveau une grappe ASA à l'aide d'ASDM (Secure Firewall 3100/4200)

Pour mettre à niveau tous les nœuds d'une grappe ASA, suivez les étapes suivantes.

Avant de commencer

- Exécutez ces étapes sur le nœud de contrôle.
- Effectuez ces étapes dans l'espace d'exécution du système pour le mode contexte multiple.
- Placez l'image ASA sur votre ordinateur de gestion local.

Procédure

Étape 1 Lancez ASDM sur le nœud *de contrôle* en vous connectant à l'adresse IP principale de la grappe.

Cette adresse IP reste toujours avec le nœud de contrôle.

Étape 2 Si vous avez précédemment défini une image ASDM autre que celle par défaut, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Dans la fenêtre principale de l'application ASDM, choisissez **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** (Configuration, Gestion de appareils, Image/Configuration du système, Image/Configuration de démarrage).
b) Pour le **chemin d'accès au fichier image ASDM**, saisissez **disk0:/asdm.bin**.
c) Cliquez sur **Apply**.

Étape 3 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel à partir de l'ordinateur local** s'affiche.

Étape 4 Cliquez sur le bouton radio **Tous les périphériques de la grappe**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 5 Dans la liste déroulante **Image à charger**, sélectionnez **ASA**.

Étape 6 Dans le champ **Chemin d'accès au fichier local**, cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 7 (Facultatif) Dans le champ **Chemin d'accès au système de fichiers flash**, saisissez le chemin d'accès au système de fichiers flash ou cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Par défaut, ce champ est prérempli avec le chemin suivant : **disk0:**/*filename*.

Étape 8 Cliquez sur **Charger une image**. Le processus de chargement peut prendre quelques minutes.

Étape 9 Vous êtes invité à définir cette image comme image ASA. Cliquez sur **Oui**.

Étape 10 Il vous est rappelé de recharger l'ASA pour utiliser la nouvelle image. Cliquez sur **OK**.

Vous quittez l'outil Mise à niveau.

Étape 11 Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Ces modifications de configuration sont automatiquement enregistrées sur les nœuds de données.

Étape 12 Notez les adresses IP de gestion individuelles pour chaque nœud dans la section **Configuration** > **Gestion des périphériques** > **Haute disponibilité et évolutivité** > **Grappe ASA** > **Membres de la grappe** afin de pouvoir connecter ASDM directement aux nœuds de données ultérieurement.

Étape 13 Mettez à niveau les nœuds de données en les rechargeant.

Remarque
Pendant le processus de mise à niveau, ne modifiez jamais le nœud de contrôle à l'aide de la page **Surveillance** > **Grappe ASA** > **Résumé de la grappe** pour forcer un nœud de données à devenir le nœud de contrôle; vous pouvez causer des problèmes de connectivité au réseau et de stabilité de grappe. Vous devez

d'abord recharger tous les nœuds de données, puis poursuivre cette procédure pour assurer une transition harmonieuse du nœud de contrôle actuel vers un nouveau nœud de contrôle.

a) Sur le nœud de contrôle, choisissez **Outils** > **Rechargement du système**.
b) Choisissez un nom de nœud de données dans la liste déroulante **Périphérique**.
c) Cliquer sur **Planifier le rechargement**.
d) Cliquez sur **Oui** pour poursuivre le rechargement.
e) Répétez l'opération pour chaque nœud de données.

   Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque nœud soit de nouveau opérationnel et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour le nœud suivant. Pour savoir quand un nœud rejoint la grappe, consultez le volet **Surveillance** > **Grappe ASA** > **Résumé de la grappe**.

Étape 14 Mettez à niveau le nœud de contrôle en le rechargeant.

a) Dans ASDM sur le nœud de contrôle, choisissez le volet **Configuration** > **Gestion des périphériques** > **Haute disponibilité et évolutivité** > **Grappe ASA** > **Configuration de grappe**.
b) Décochez la case **Participer à la grappe ASA**, puis cliquez sur **Appliquer**.

   Vous êtes invité à quitter ASDM.

c) Attendez jusqu'à 5 minutes qu'un nouveau nœud de contrôle soit sélectionné et que le trafic se stabilise.

   Lorsque l'ancien nœud de contrôle rejoint la grappe, il devient un nœud de données.

d) Reconnectez ASDM à l'ancien nœud de contrôle en vous connectant à son adresse IP de gestion *individuelle* que vous avez notée plus tôt.

   L'adresse IP de la grappe principale appartient maintenant au nouveau nœud de contrôle. Cet ancien nœud de contrôle est toujours accessible sur son adresse IP de gestion individuelle.

e) Choisissez **Outils** > **Rechargement du système**.
f) Cliquez sur le bouton radio **Recharger sans enregistrer la configuration en cours**.

   Il ne faut pas sauvegarder la configuration. Lorsque cette unité sera rechargée, vous voudrez que la mise en grappe soit activée sur ce nœud.

g) Cliquer sur **Planifier le rechargement**.
h) Cliquez sur **Oui** pour poursuivre le rechargement.

   Vous êtes invité à quitter ASDM. Redémarrez ASDM sur l'adresse IP de la grappe principale. Vous vous reconnecterez au nouveau nœud de contrôle.

Mettre à niveau le Firepower 4100/9300

Ce document décrit comment mettre à niveau l'ASA sur le Firepower 4100/9300.

Mettre à niveau FXOS et un périphérique autonome ASA ou une grappe intra-châssis

Utilisez l'interface de ligne de commande de FXOS ou Firepower Chassis Manager pour mettre à niveau FXOS et un périphérique ASA autonome ou une grappe intra-châssis ASA sur un Firepower 9300.

Mettre à niveau FXOS et un périphérique autonome ASA ou une grappe intra-châssis à l'aide de Cisco Secure Firewall Chassis Manager

Le processus de mise à niveau peut prendre jusqu'à 45 minutes. Le trafic ne traversera pas le périphérique pendant la mise à niveau. Veuillez planifier vos activités de mise à niveau en conséquence.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez les paquets FXOS et ASA vers lesquels vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et ASA.

Procédure

Étape 1 Dans Cisco Secure Firewall chassis manager, sélectionnez **Système** > **Mises à jour**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.

Étape 2 Chargez la nouvelle image groupée de la plateforme FXOS et l'image logicielle ASA :

a) Cliquez sur **Charger une image**.
b) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
c) Cliquez sur **Upload** (charger).
L'image sélectionnée est chargée sur le châssis.

Étape 3 Une fois que la nouvelle image groupée de plateforme FXOS a été chargée, cliquez sur l'icône **Mise à niveau** de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

Étape 4 Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

Étape 5 Firepower Chassis Manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide de Interface de ligne de commande FXOS (voir Surveiller l'avancement de la mise à niveau, à la page 127).

Étape 6 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 7 Choisissez **Périphériques logiques**.
La page **Périphériques logiques** s'ouvre et affiche la liste des périphériques logiques configurés sur le châssis.

Étape 8 Pour chaque périphérique logique ASA que vous souhaitez mettre à niveau :

a) Cliquez sur l'icône **Définir la version** du périphérique logique que vous souhaitez mettre à jour pour ouvrir la boîte de dialogue **Mettre à jour la version de l'image**.

b) Pour la **nouvelle version**, choisissez la version du logiciel vers laquelle vous souhaitez effectuer la mise à niveau.

c) Cliquez sur **OK**.

Étape 9 Une fois que le processus de mise à niveau est terminé, vérifiez que les applications sont en ligne et ont bien été mises à niveau :

a) Choisissez **Périphériques logiques**.

b) Vérifiez la version de l'application et l'état opérationnel.

Mettre à niveau FXOS et un périphérique autonome ASA ou une grappe intra-châssis à l'aide de l'interface de ligne de commande de FXOS

Le processus de mise à niveau peut prendre jusqu'à 45 minutes. Le trafic ne traversera pas le périphérique pendant la mise à niveau. Veuillez planifier vos activités de mise à niveau en conséquence.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez les paquets FXOS et ASA vers lesquels vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et ASA.
- Chargez les informations suivantes dont vous aurez besoin pour télécharger les images logicielles sur le châssis :
  - L'adresse IP et les informations d'authentification du serveur à partir duquel vous copiez les images.
  - Noms complets des fichiers image.

Procédure

Étape 1 Connectez-vous au Interface de ligne de commande FXOS.

Étape 2 Téléchargez la nouvelle image groupée de la plateforme FXOS sur le châssis :

a) Entrez en mode micrologiciel :

scope firmware

b) Téléchargez l'image logicielle de l'ensemble de la plateforme FXOS :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur/chemin/nom_de_l_image*
- **scp**://*nom_d_utilisateur@serveur/chemin/nom_de_l_image*

- **sftp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **tftp**://*serveur***:***numéro_de_port*/*chemin*/*nom_de_l_image*

c) Pour surveiller le processus de téléchargement :

scope download-task *nom_de_l_image*

show detail

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 3 Une fois que la nouvelle image groupée de la plateforme FXOS a été téléchargée, mettez à niveau l'offre groupée FXOS :

a) Si nécessaire, revenez au mode micrologiciel :

up

b) Notez le numéro de version de l'ensemble de la plateforme FXOS que vous installez :

show package

c) Passez en mode d'installation automatique :

scope auto-install

d) Installez l'ensemble de la plateforme FXOS :

install platform platform-vers *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez, par exemple, la version 2.3(1.58).

e) Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

Saisissez **yes** pour confirmer que vous souhaitez procéder à la vérification.

f) Saisissez **yes** pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

g) Pour surveiller le processus de mise à niveau, consultez Surveiller l'avancement de la mise à niveau, à la page 127.

Étape 4 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 5 Téléchargez la nouvelle image logicielle ASA sur le châssis :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Entrez le mode des logiciels d'application :

scope app-software

c) Téléchargez l'image logicielle du périphérique logique :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*
- **tftp**://*serveur*:*numéro_de_port*/*chemin*

d) Pour surveiller le processus de téléchargement :

show download-task

e) Pour afficher les applications téléchargées :

up

show app

Notez la version ASA pour le paquet que vous avez téléchargé. Vous devrez utiliser la chaîne de version exacte pour activer l'application à une étape ultérieure.

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server              Userid          State
    ----------------------------- ---------- ------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1         user            Downloaded

Firepower-chassis /ssa/app-software # up
```

```
Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Étape 6 Pour chaque périphérique logique ASA que vous souhaitez mettre à niveau :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Définissez la portée au module de sécurité que vous mettez à jour :

scope slot*slot_number*

c) Définissez la portée de l'application ASA :

scope app-instance asa *instance_name*

d) Définissez la version de démarrage sur la nouvelle version du logiciel ASA :

set startup-version *version_number*

Étape 7 Validez la configuration :

commit-buffer

Validez la transaction dans la configuration du système. L'image de l'application est mise à jour et l'application redémarre.

Étape 8 Pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées, consultez Vérifier l'installation, à la page 128.

Mettre à niveau FXOS et une paire de basculements ASA actif/de secours

Utilisez l'interface de ligne de commande de FXOS ou Firepower Chassis Manager pour mettre à niveau FXOS et une paire de basculements ASA actif/de secours.

Mettre à niveau FXOS et une paire de basculements ASA actif/de secours à l'aide de Cisco Secure Firewall Chassis Manager

Le processus de mise à niveau peut prendre jusqu'à 45 minutes par châssis. Veuillez planifier vos activités de mise à niveau en conséquence.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Vous devez déterminer quelle unité est active et laquelle est considérée comme étant de secours : connectez ASDM à l'adresse IP ASA active. L'unité active est toujours propriétaire de l'adresse IP active. Ensuite,

sélectionnez **Surveillance** > **Propriétés** > **Basculement** > **État** pour afficher la priorité de cette unité (principale ou secondaire) afin de savoir à quelle unité vous êtes connecté.

- Téléchargez les paquets FXOS et ASA vers lesquels vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et ASA.

Procédure

Étape 1 Sur le châssis qui contient le périphérique logique ASA *de secours*, chargez la nouvelle image groupée de la plateforme FXOS ainsi que l'image logicielle ASA :

a) Dans Cisco Secure Firewall chassis manager, sélectionnez **Système** > **Mises à jour**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.
b) Cliquez sur **Charger une image**.
c) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
d) Cliquez sur **Upload** (charger).
L'image sélectionnée est chargée sur le châssis.

Étape 2 Une fois que la nouvelle image groupée de la plateforme FXOS a été chargée, mettez à niveau l'ensemble FXOS sur le châssis qui contient le périphérique logique ASA *de secours* :

a) Cliquez sur l'icône **Mise à niveau** de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

b) Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

Étape 3 Cisco Secure Firewall chassis manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide de Interface de ligne de commande FXOS (voir Surveiller l'avancement de la mise à niveau, à la page 127).

Étape 4 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 5 Mettez à niveau l'image du périphérique logique ASA :

a) Choisissez **Périphériques logiques** pour ouvrir la page Périphériques logiques.
La page **Périphériques logiques** s'ouvre et affiche la liste des périphériques logiques configurés sur le châssis.
b) Cliquez sur l'icône **Définir la version** du périphérique logique que vous souhaitez mettre à jour pour ouvrir la boîte de dialogue **Mettre à jour la version de l'image**.
c) Pour la **nouvelle version**, choisissez la version du logiciel vers laquelle vous souhaitez effectuer la mise à jour.
d) Cliquez sur **OK**.

Étape 6 Une fois que le processus de mise à niveau est terminé, vérifiez que les applications sont en ligne et ont bien été mises à niveau :

a) Choisissez **Périphériques logiques**.
b) Vérifiez la version de l'application et l'état opérationnel.

Étape 7 Faites de l'unité que vous venez de mettre à niveau l'unité *active* afin que le trafic flux de trafic vers l'unité mise à niveau :

a) Lancez ASDM sur l'unité *de secours* en vous connectant à l'adresse IP de l'ASA de secours.
b) Forcez l'unité de secours à devenir active en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Faire passer en groupe actif**.

Étape 8 Sur le châssis qui contient le nouveau périphérique logique ASA *de secours*, chargez la nouvelle image groupée de la plateforme FXOS ainsi que l'image logicielle ASA :

a) Dans Cisco Secure Firewall chassis manager, sélectionnez **Système** > **Mises à jour**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.
b) Cliquez sur **Charger une image**.
c) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
d) Cliquez sur **Upload** (charger).
L'image sélectionnée est chargée sur le châssis.

Étape 9 Une fois que la nouvelle image groupée de la plateforme FXOS a été chargée, mettez à niveau l'ensemble FXOS sur le châssis qui contient le nouveau périphérique logique ASA *de secours* :

a) Cliquez sur l'icône **Mise à niveau** de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

b) Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

Étape 10 Cisco Secure Firewall chassis manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide de Interface de ligne de commande FXOS (voir Surveiller l'avancement de la mise à niveau, à la page 127).

Étape 11 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 12 Mettez à niveau l'image du périphérique logique ASA :

a) Choisissez **Périphériques logiques**.
La page **Périphériques logiques** s'ouvre et affiche la liste des périphériques logiques configurés sur le châssis. Si aucun périphérique logique n'a été configuré, un message l'indiquant s'affiche à la place.
b) Cliquez sur l'icône **Définir la version** du périphérique logique que vous souhaitez mettre à jour pour ouvrir la boîte de dialogue **Mettre à jour la version de l'image**.
c) Pour la **nouvelle version**, choisissez la version du logiciel vers laquelle vous souhaitez effectuer la mise à jour.
d) Cliquez sur **OK**.

Étape 13 Une fois que le processus de mise à niveau est terminé, vérifiez que les applications sont en ligne et ont bien été mises à niveau :

a) Choisissez **Périphériques logiques**.
b) Vérifiez la version de l'application et l'état opérationnel.

Étape 14 (Facultatif) Faites de l'unité que vous venez de mettre à niveau l'unité *active* comme elle l'était avant la mise à niveau :

a) Lancez ASDM sur l'unité *de secours* en vous connectant à l'adresse IP de l'ASA de secours.
b) Forcez l'unité de secours à devenir active en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Faire passer en groupe actif**.

Mettre à niveau FXOS et une paire de basculements ASA actif/de secours à l'aide de l'interface de ligne de commande de FXOS

Le processus de mise à niveau peut prendre jusqu'à 45 minutes par châssis. Veuillez planifier vos activités de mise à niveau en conséquence.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Vous devez déterminer quelle unité est active et laquelle est considérée comme étant de secours : connectez-vous à la console ASA sur le châssis et saisissez la commande **show failover** pour afficher l'état Actif/De secours de l'unité.
- Téléchargez les paquets FXOS et ASA vers lesquels vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et ASA.
- Chargez les informations suivantes dont vous aurez besoin pour télécharger les images logicielles sur le châssis :
  - L'adresse IP et les informations d'authentification du serveur à partir duquel vous copiez l'image.
  - Nom complet du fichier image.

Procédure

Étape 1 Sur le châssis qui contient le périphérique logique ASA *de secours*, téléchargez la nouvelle image groupée de la plateforme FXOS :

a) Connectez-vous au Interface de ligne de commande FXOS.
b) Entrez en mode micrologiciel :

scope firmware

c) Téléchargez l'image logicielle de l'ensemble de la plateforme FXOS :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur/chemin/nom_de_l_image*
- **scp**://*nom_d_utilisateur@serveur/chemin/nom_de_l_image*
- **sftp**://*nom_d_utilisateur@serveur/chemin/nom_de_l_image*

- **tftp**://*serveur* **:** *numéro_de_port* / *chemin* / *nom_de_l_image*

d) Pour surveiller le processus de téléchargement :

scope download-task *nom_de_l_image*

show detail

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 2 Une fois que la nouvelle image groupée de la plateforme FXOS a été téléchargée, mettez à niveau l'offre groupée FXOS :

a) Si nécessaire, revenez au mode micrologiciel :

up

b) Notez le numéro de version de l'ensemble de la plateforme FXOS que vous installez :

show package

c) Passez en mode d'installation automatique :

scope auto-install

d) Installez l'ensemble de la plateforme FXOS :

install platform platform-vers *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez, par exemple, la version 2.3(1.58).

e) Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

Saisissez **yes** pour confirmer que vous souhaitez procéder à la vérification.

f) Saisissez **yes** pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

g) Pour surveiller le processus de mise à niveau, consultez Surveiller l'avancement de la mise à niveau, à la page 127.

Étape 3 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 4 Téléchargez la nouvelle image logicielle ASA sur le châssis :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Entrez le mode des logiciels d'application :

scope app-software

c) Téléchargez l'image logicielle du périphérique logique :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*
- **tftp**://*serveur*:*numéro_de_port*/*chemin*

d) Pour surveiller le processus de téléchargement :

show download-task

e) Pour afficher les applications téléchargées :

up

show app

Notez la version ASA pour le paquet que vous avez téléchargé. Vous devrez utiliser la chaîne de version exacte pour activer l'application à une étape ultérieure.

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server              Userid          State
    ----------------------------- ---------- ------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1         user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app
```

```
Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Étape 5 Mettez à niveau l'image du périphérique logique ASA :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Définissez la portée au module de sécurité que vous mettez à jour :

scope slot*slot_number*

c) Définissez la portée de l'application ASA :

scope app-instance asa *instance_name*

d) Définissez la version de démarrage sur la version que vous souhaitez mettre à jour :

set startup-version *version_number*

e) Validez la configuration :

commit-buffer

Validez la transaction dans la configuration du système. L'image de l'application est mise à jour et l'application redémarre.

Étape 6 Pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées, consultez Vérifier l'installation, à la page 128.

Étape 7 Faites de l'unité que vous venez de mettre à niveau l'unité *active* afin que le trafic flux de trafic vers l'unité mise à niveau :

a) Sur le châssis qui contient le périphérique logique ASA de secours, connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module *slot_number* {**console** | **telnet**}

Pour vous connecter au moteur de sécurité d'un périphérique qui ne prend pas en charge plusieurs modules de sécurité, utilisez toujours **1** comme *slot_number*.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connectez-vous à la console d'application.

connect asa

Exemple :

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Activez cette unité :

failover active

d) Enregistrez la configuration :

write memory

e) Vérifiez que l'unité est active :

show failover

Étape 8 Quittez la console d'application pour accéder à l'interface de ligne de commande du module FXOS.

Saisissez **Ctrl-a, d**

Étape 9 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Étape 10 Sur le châssis qui contient le nouveau périphérique logique ASA *de secours*, téléchargez la nouvelle image groupée de la plateforme FXOS :

a) Connectez-vous au Interface de ligne de commande FXOS.

b) Entrez en mode micrologiciel :

scope firmware

c) Téléchargez l'image logicielle de l'ensemble de la plateforme FXOS :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **tftp**://*serveur***:***numéro_de_port*/*chemin*/*nom_de_l_image*

d) Pour surveiller le processus de téléchargement :

scope download-task *nom_de_l_image*

show detail

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 11 Une fois que la nouvelle image groupée de la plateforme FXOS a été téléchargée, mettez à niveau l'offre groupée FXOS :

a) Si nécessaire, revenez au mode micrologiciel :

up

b) Notez le numéro de version de l'ensemble de la plateforme FXOS que vous installez :

show package

c) Passez en mode d'installation automatique :

scope auto-install

d) Installez l'ensemble de la plateforme FXOS :

install platform platform-vers *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez, par exemple, la version 2.3(1.58).

e) Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

Saisissez **yes** pour confirmer que vous souhaitez procéder à la vérification.

f) Saisissez **yes** pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

g) Pour surveiller le processus de mise à niveau, consultez Surveiller l'avancement de la mise à niveau, à la page 127.

Étape 12 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 13 Téléchargez la nouvelle image logicielle ASA sur le châssis :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Entrez le mode des logiciels d'application :

scope app-software

c) Téléchargez l'image logicielle du périphérique logique :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*
- **tftp**://*serveur*:*numéro_de_port*/*chemin*

d) Pour surveiller le processus de téléchargement :

show download-task

e) Pour afficher les applications téléchargées :

up

show app

Notez la version ASA pour le paquet que vous avez téléchargé. Vous devrez utiliser la chaîne de version exacte pour activer l'application à une étape ultérieure.

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server              Userid          State
    ----------------------------- ---------- ------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1         user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app
```

```
Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Étape 14 Mettez à niveau l'image du périphérique logique ASA :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Définissez la portée au module de sécurité que vous mettez à jour :

scope slot*slot_number*

c) Définissez la portée de l'application ASA :

scope app-instance asa *instance_name*

d) Définissez la version de démarrage sur la version que vous souhaitez mettre à jour :

set startup-version *version_number*

e) Validez la configuration :

commit-buffer

Validez la transaction dans la configuration du système. L'image de l'application est mise à jour et l'application redémarre.

Étape 15 Pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées, consultez Vérifier l'installation, à la page 128.

Étape 16 (Facultatif) Faites de l'unité que vous venez de mettre à niveau l'unité *active* comme elle l'était avant la mise à niveau :

a) Sur le châssis qui contient le périphérique logique ASA de secours, connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module *slot_number* {**console** | **telnet**}

Pour vous connecter au moteur de sécurité d'un périphérique qui ne prend pas en charge plusieurs modules de sécurité, utilisez toujours **1** comme *slot_number*.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connectez-vous à la console d'application.

connect asa

Exemple :

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Activez cette unité :

failover active

d) Enregistrez la configuration :

write memory

e) Vérifiez que l'unité est active :

show failover

Mettre à niveau FXOS et une paire de basculements ASA actif/actif

Utilisez l'interface de ligne de commande de FXOS ou Firepower Chassis Manager pour mettre à niveau FXOS et une paire de basculements ASA actif/actif.

Mettre à niveau FXOS et une paire de basculements ASA actif/actif à l'aide de Cisco Secure Firewall Chassis Manager

Le processus de mise à niveau peut prendre jusqu'à 45 minutes par châssis. Veuillez planifier vos activités de mise à niveau en conséquence.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Vous devez déterminer quelle unité est l'unité principale : connectez ASDM, puis sélectionnez **Surveillance** > **Propriétés** > **Basculement** > **État** pour afficher la priorité de cette unité (principale ou secondaire) afin de savoir à quelle unité vous êtes connecté.
- Téléchargez les paquets FXOS et ASA vers lesquels vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et ASA.

Procédure

Étape 1 Activez les deux groupes de basculement sur l'unité *principale*.

a) Lancez ASDM sur l'unité *principale* (ou l'unité avec le groupe de basculement 1 actif) en vous connectant à l'adresse de gestion dans le groupe de basculement 1.

b) Choisissez **Surveillance** > **Basculement** > **Groupe de basculement 2**, puis cliquez sur **Faire passer en groupe actif**.
c) Restez connecté à ASDM sur cette unité pour les étapes ultérieures.

Étape 2 Sur le châssis qui contient le périphérique logique ASA *secondaire*, chargez la nouvelle image groupée de la plateforme FXOS ainsi que l'image logicielle ASA :

a) Connectez-vous au Cisco Secure Firewall chassis manager sur l'unité *secondaire*.
b) Choisissez **Système** > **Mises à jour**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.
c) Cliquez sur **Charger une image**.
d) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
e) Cliquez sur **Upload** (charger).
L'image sélectionnée est chargée sur le châssis.

Étape 3 Une fois que la nouvelle image groupée de la plateforme FXOS a été chargée, mettez à niveau l'ensemble FXOS sur le châssis qui contient le périphérique logique ASA *secondaire* :

a) Cliquez sur l'icône **Mise à niveau** de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

b) Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

Étape 4 Cisco Secure Firewall chassis manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide de Interface de ligne de commande FXOS (voir Surveiller l'avancement de la mise à niveau, à la page 127).

Étape 5 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 6 Mettez à niveau l'image du périphérique logique ASA :

a) Choisissez **Périphériques logiques**.
La page **Périphériques logiques** s'ouvre et affiche la liste des périphériques logiques configurés sur le châssis.
b) Cliquez sur l'icône **Définir la version** du périphérique logique que vous souhaitez mettre à jour pour ouvrir la boîte de dialogue **Mettre à jour la version de l'image**.
c) Pour la **nouvelle version**, choisissez la version du logiciel vers laquelle vous souhaitez effectuer la mise à jour.
d) Cliquez sur **OK**.

Étape 7 Une fois que le processus de mise à niveau est terminé, vérifiez que les applications sont en ligne et ont bien été mises à niveau :

a) Choisissez **Périphériques logiques**.
b) Vérifiez la version de l'application et l'état opérationnel.

Étape 8 Activez les deux groupes de basculement sur l'unité *secondaire*.

a) Lancez ASDM sur l'unité *principale* (ou l'unité avec le groupe de basculement 1 actif) en vous connectant à l'adresse de gestion dans le groupe de basculement 1.

b) Choisissez **Surveillance** > **Basculement** > **Groupe de basculement 1**, puis cliquez sur **Faire passer en groupe de secours**.
c) Choisissez **Surveillance** > **Basculement** > **Groupe de basculement 2**, puis cliquez sur **Faire passer en groupe de secours**.

ASDM se reconnectera automatiquement à l'adresse IP du groupe de basculement 1 sur l'unité secondaire.

Étape 9 Sur le châssis qui contient le périphérique logique ASA *principal*, chargez la nouvelle image groupée de la plateforme FXOS ainsi que l'image logicielle ASA :

a) Connectez-vous au Cisco Secure Firewall chassis manager de l'unité *principale*.
b) Choisissez **Système** > **Mises à jour**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.
c) Cliquez sur **Upload Image**(télécharger une image) pour ouvrir la boîte de dialogue pour télécharger une image (Upload Image).
d) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
e) Cliquez sur **Upload** (charger).
Le paquet sélectionné est chargé sur le châssis.
f) Pour certaines images logicielles, vous recevrez un contrat de licence d'utilisateur final après le téléchargement de l'image. Suivez les messages-guides du système pour accepter le contrat de licence d'utilisateur final.

Étape 10 Une fois que la nouvelle image groupée de la plateforme FXOS a été chargée, mettez à niveau l'ensemble FXOS sur le châssis qui contient le périphérique logique ASA *principal* :

a) Cliquez sur l'icône **Mise à niveau** de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

b) Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

Étape 11 Cisco Secure Firewall chassis manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide de Interface de ligne de commande FXOS (voir Surveiller l'avancement de la mise à niveau, à la page 127).

Étape 12 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 13 Mettez à niveau l'image du périphérique logique ASA :

a) Choisissez **Périphériques logiques**.
La page **Périphériques logiques** s'ouvre et affiche la liste des périphériques logiques configurés sur le châssis.
b) Cliquez sur l'icône **Définir la version** du périphérique logique que vous souhaitez mettre à jour pour ouvrir la boîte de dialogue **Mettre à jour la version de l'image**.
c) Pour la **nouvelle version**, choisissez la version du logiciel vers laquelle vous souhaitez effectuer la mise à jour.
d) Cliquez sur **OK**.

Étape 14 Une fois que le processus de mise à niveau est terminé, vérifiez que les applications sont en ligne et ont bien été mises à niveau :

a) Choisissez **Périphériques logiques**.

b) Vérifiez la version de l'application et l'état opérationnel.

Étape 15 Si les groupes de basculement sont configurés avec la préemption activée, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé. Si les groupes de basculement ne sont pas configurés avec la préemption activée, vous pouvez les rétablir à l'état actif sur leurs unités désignées à l'aide du volet ASDM **Surveillance > Basculement > Groupe de basculement #**.

Mettre à niveau FXOS et une paire de basculements ASA actif/actif à l'aide de l'interface de ligne de commande de FXOS

Le processus de mise à niveau peut prendre jusqu'à 45 minutes par châssis. Veuillez planifier vos activités de mise à niveau en conséquence.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Vous devez déterminer quelle unité est principale : connectez-vous à la console ASA sur le châssis et saisissez la commande **show failover** pour afficher l'état et la priorité de l'unité (principale ou secondaire).
- Téléchargez les paquets FXOS et ASA vers lesquels vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et ASA.
- Chargez les informations suivantes dont vous aurez besoin pour télécharger les images logicielles sur le châssis :
  - L'adresse IP et les informations d'authentification du serveur à partir duquel vous copiez l'image.
  - Nom complet du fichier image.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de FXOS sur l'unité *secondaire*, à partir du port de console (méthode préférée) ou à l'aide du protocole SSH.

Étape 2 Activez les deux groupes de basculement sur l'unité principale.

a) Connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module *slot_number* {**console** | **telnet**}

Pour vous connecter au moteur de sécurité d'un périphérique qui ne prend pas en charge plusieurs modules de sécurité, utilisez toujours **1** comme *slot_number*.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
```

```
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connectez-vous à la console d'application.

connect asa

Exemple :

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Activez les deux groupes de basculement sur l'unité principale.

enable

Le mot de passe d'activation est vide par défaut.

no failover active group 1

no failover active group 2

Exemple :

```
asa> enable
Password: <blank>
asa# no failover active group 1
asa# no failover active group 2
```

Étape 3 Quittez la console d'application pour accéder à l'interface de ligne de commande du module FXOS.

Saisissez **Ctrl-a, d**

Étape 4 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Étape 5 Sur le châssis qui contient le périphérique logique ASA *secondaire*, téléchargez la nouvelle image groupée de la plateforme FXOS ainsi que l'image logicielle ASA :

a) Connectez-vous au Interface de ligne de commande FXOS.

b) Entrez en mode micrologiciel :

scope firmware

c) Téléchargez l'image logicielle de l'ensemble de la plateforme FXOS :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **tftp**://*serveur***:***numéro_de_port*/*chemin*/*nom_de_l_image*

d) Pour surveiller le processus de téléchargement :

scope download-task *nom_de_l_image*

show detail

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 6 Une fois que la nouvelle image groupée de la plateforme FXOS a été téléchargée, mettez à niveau l'offre groupée FXOS :

a) Si nécessaire, revenez au mode micrologiciel :

top

scope firmware

b) Notez le numéro de version de l'ensemble de la plateforme FXOS que vous installez :

show package

c) Passez en mode d'installation automatique :

scope auto-install

d) Installez l'ensemble de la plateforme FXOS :

install platform platform-vers *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez, par exemple, la version 2.3(1.58).

e) Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

Saisissez **yes** pour confirmer que vous souhaitez procéder à la vérification.

f) Saisissez **yes** pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

g) Pour surveiller le processus de mise à niveau, consultez Surveiller l'avancement de la mise à niveau, à la page 127.

Étape 7 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 8 Téléchargez la nouvelle image logicielle ASA sur le châssis :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Entrez le mode des logiciels d'application :

scope app-software

c) Téléchargez l'image logicielle du périphérique logique :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*
- tftp://*serveur*:*numéro_de_port*/*chemin*

d) Pour surveiller le processus de téléchargement :

show download-task

e) Pour afficher les applications téléchargées :

up

show app

Notez la version ASA pour le paquet que vous avez téléchargé. Vous devrez utiliser la chaîne de version exacte pour activer l'application à une étape ultérieure.

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Étape 9 Mettez à niveau l'image du périphérique logique ASA :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Définissez la portée au module de sécurité que vous mettez à jour :

scope slot*slot_number*

c) Définissez la portée de l'application ASA :

scope app-instance asa *instance_name*

d) Définissez la version de démarrage sur la version que vous souhaitez mettre à jour :

set startup-version *version_number*

e) Validez la configuration :

commit-buffer

Validez la transaction dans la configuration du système. L'image de l'application est mise à jour et l'application redémarre.

Étape 10 Pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées, consultez Vérifier l'installation, à la page 128.

Étape 11 Activez les deux groupes de basculement sur l'unité *secondaire*.

a) Connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module *slot_number* {**console** | **telnet**}

Pour vous connecter au moteur de sécurité d'un périphérique qui ne prend pas en charge plusieurs modules de sécurité, utilisez toujours **1** comme *slot_number*.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connectez-vous à la console d'application.

connect asa

Exemple :

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Activez les deux groupes de basculement sur l'unité *secondaire*.

enable

Le mot de passe d'activation est vide par défaut.

failover active group 1

failover active group 2

Exemple :

```
asa> enable
Password: <blank>
asa# failover active group 1
asa# failover active group 2
```

Étape 12 Quittez la console d'application pour accéder à l'interface de ligne de commande du module FXOS.

Saisissez **Ctrl-a, d**

Étape 13 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Étape 14 Sur le châssis qui contient le périphérique logique ASA *principal*, téléchargez la nouvelle image groupée de la plateforme FXOS ainsi que l'image logicielle ASA :

a) Connectez-vous au Interface de ligne de commande FXOS.
b) Entrez en mode micrologiciel :

scope firmware

c) Téléchargez l'image logicielle de l'ensemble de la plateforme FXOS :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- tftp://*serveur***:***numéro_de_port*/*chemin*/*nom_de_l_image*

d) Pour surveiller le processus de téléchargement :

scope download-task *nom_de_l_image*

show detail

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 15 Une fois que la nouvelle image groupée de la plateforme FXOS a été téléchargée, mettez à niveau l'offre groupée FXOS :

a) Si nécessaire, revenez au mode micrologiciel :

up

b) Notez le numéro de version de l'ensemble de la plateforme FXOS que vous installez :

show package

c) Passez en mode d'installation automatique :

scope auto-install

d) Installez l'ensemble de la plateforme FXOS :

install platform platform-vers *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez, par exemple, la version 2.3(1.58).

e) Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

Saisissez **yes** pour confirmer que vous souhaitez procéder à la vérification.

f) Saisissez **yes** pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

g) Pour surveiller le processus de mise à niveau, consultez Surveiller l'avancement de la mise à niveau, à la page 127.

Étape 16 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 17 Téléchargez la nouvelle image logicielle ASA sur le châssis :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Entrez le mode des logiciels d'application :

scope app-software

c) Téléchargez l'image logicielle du périphérique logique :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*
- **tftp**://*serveur*:*numéro_de_port*/*chemin*

d) Pour surveiller le processus de téléchargement :

show download-task

e) Pour afficher les applications téléchargées :

up

show app

Notez la version ASA pour le paquet que vous avez téléchargé. Vous devrez utiliser la chaîne de version exacte pour activer l'application à une étape ultérieure.

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Étape 18 Mettez à niveau l'image du périphérique logique ASA :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Définissez la portée au module de sécurité que vous mettez à jour :

scope slot*slot_number*

c) Définissez la portée de l'application ASA :

scope app-instance asa *instance_name*

d) Définissez la version de démarrage sur la version que vous souhaitez mettre à jour :

set startup-version *version_number*

e) Validez la configuration :

commit-buffer

Validez la transaction dans la configuration du système. L'image de l'application est mise à jour et l'application redémarre.

Étape 19 Pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées, consultez Vérifier l'installation, à la page 128.

Étape 20 Si les groupes de basculement sont configurés avec la préemption activée, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé. Si les groupes de basculement ne sont pas configurés avec la préemption activée, vous pouvez les rétablir à l'état actif sur leurs unités désignées à l'aide du volet ASDM **Surveillance > Basculement > Groupe de basculement #**.

Mettre à niveau FXOS et une grappe inter-châssis ASA

Utilisez l'interface de ligne de commande de FXOS ou Firepower Chassis Manager pour mettre à niveau FXOS et ASA sur tous les châssis d'une grappe inter-châssis.

Mettre à niveau FXOS et une grappe inter-châssis ASA à l'aide de Cisco Secure Firewall Chassis Manager

Le processus de mise à niveau peut prendre jusqu'à 45 minutes par châssis. Veuillez planifier vos activités de mise à niveau en conséquence.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez les paquets FXOS et ASA vers lesquels vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et ASA.

Procédure

Étape 1 Déterminez quel châssis comporte le nœud de contrôle. Vous mettrez ce châssis à niveau en dernier.

a) Connectez-vous à Cisco Secure Firewall chassis manager.
b) Choisissez **Périphériques logiques**.
c) Cliquez sur le signe plus (+) pour afficher les attributs des modules de sécurité inclus dans la grappe.
d) Vérifiez que le nœud de contrôle se trouve sur ce châssis. Il devrait y avoir une instance d'ASA où le paramètre **CLUSTER-ROLE** est défini sur « Control ».

Étape 2 Connectez-vous à Cisco Secure Firewall chassis manager sur un châssis de la grappe qui **ne comporte pas de nœud de contrôle**.

Étape 3 Chargez la nouvelle image groupée de la plateforme FXOS et l'image logicielle ASA :

a) Dans Cisco Secure Firewall chassis manager, sélectionnez **Système** > **Mises à jour**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.
b) Cliquez sur **Charger une image**.
c) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
d) Cliquez sur **Upload** (charger).
L'image sélectionnée est chargée sur le châssis.
e) Attendez que les images soient correctement chargées avant de continuer.

Étape 4 Mettez à niveau l'ensemble FXOS :

a) Sélectionnez **Système** > **Mises à jour**.
b) Cliquez sur l'icône **Mise à niveau** de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

c) Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

Étape 5 Cisco Secure Firewall chassis manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide de Interface de ligne de commande FXOS (voir Surveiller l'avancement de la mise à niveau, à la page 127).

Étape 6 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 7 Mettez à niveau l'image du périphérique logique ASA sur chaque module de sécurité :

a) Choisissez **Périphériques logiques**.
La page **Périphériques logiques** s'ouvre et affiche la liste des périphériques logiques configurés sur le châssis.

b) Cliquez sur l'icône **Définir la version** du périphérique logique que vous souhaitez mettre à jour pour ouvrir la boîte de dialogue **Mettre à jour la version de l'image**.

c) Pour la **nouvelle version**, choisissez la version du logiciel vers laquelle vous souhaitez effectuer la mise à jour.

d) Cliquez sur **OK**.

Étape 8 Une fois que le processus de mise à niveau est terminé, vérifiez que les applications sont en ligne et ont bien été mises à niveau :

a) Choisissez **Périphériques logiques**.

b) Vérifiez la version de l'application et l'état opérationnel.

Étape 9 Répétez les étapes Étape 2, à la page 122–Étape 8, à la page 123 pour tous les châssis restants de la grappe qui ne disposent pas de nœud de contrôle.

Étape 10 Une fois que tous les châssis de la grappe qui ne disposent pas de nœud de contrôle ont été mis à niveau, répétez les étapes Étape 2, à la page 122–Étape 8, à la page 123 sur le châssis **avec le nœud de contrôle**. Un nouveau nœud de contrôle sera choisi dans l'un des châssis précédemment mis à niveau.

Étape 11 Pour le mode de mise en grappe VPN distribuée, une fois que la grappe est stable, redistribuez les sessions actives entre tous les modules de la grappe à l'aide de la console ASA sur l'unité de contrôle.

cluster redistribute vpn-sessiondb

Prochaine étape

Définissez l'ID de site de châssis. Pour en savoir plus sur la définition de l'ID de site du châssis, consultez la rubrique sur la mise en grappe intersite dans Déploiement d'une grappe pour ASA sur le Firepower 4100/9300 pour l'évolutivité et la haute disponibilité sur Cisco.com.

Mettre à niveau FXOS et une grappe inter-châssis ASA à l'aide de l'interface de ligne de commande de FXOS

Le processus de mise à niveau peut prendre jusqu'à 45 minutes par châssis. Veuillez planifier vos activités de mise à niveau en conséquence.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez les paquets FXOS et ASA vers lesquels vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et ASA.
- Chargez les informations suivantes dont vous aurez besoin pour télécharger les images logicielles sur le châssis :
  - L'adresse IP et les informations d'authentification du serveur à partir duquel vous copiez l'image.
  - Nom complet du fichier image.

Procédure

Étape 1 Déterminez quel châssis comporte le nœud de contrôle. Vous mettrez ce châssis à niveau en dernier.

a) Connectez-vous au Interface de ligne de commande FXOS.

b) Vérifiez que le nœud de contrôle se trouve sur ce châssis. Il devrait y avoir une instance ASA avec le rôle de grappe défini sur « Control » :

scope ssa

show app-instance

Étape 2 Connectez-vous au Interface de ligne de commande FXOS sur un châssis de la grappe qui **ne comporte pas de nœud de contrôle**.

Étape 3 Téléchargez la nouvelle image groupée de la plateforme FXOS sur le châssis :

a) Entrez en mode micrologiciel :

scope firmware

b) Téléchargez l'image logicielle de l'ensemble de la plateforme FXOS :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*/*nom_de_l_image*
- **tftp**://*serveur***:***numéro_de_port*/*chemin*/*nom_de_l_image*

c) Pour surveiller le processus de téléchargement :

scope download-task *nom_de_l_image*

show detail

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
```

```
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 4 Mettez à niveau l'ensemble FXOS :

a) Si nécessaire, revenez au mode micrologiciel :

top

scope firmware

b) Notez le numéro de version de l'ensemble de la plateforme FXOS que vous installez :

show package

c) Passez en mode d'installation automatique :

scope auto-install

d) Installez l'ensemble de la plateforme FXOS :

install platform platform-vers *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez, par exemple, la version 2.3(1.58).

e) Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau. Tant que la version de l'ASA est répertoriée comme pouvant être mise à niveau dans le tableau de compatibilité, vous pouvez ignorer ces avertissements.

Saisissez **yes** pour confirmer que vous souhaitez procéder à la vérification.

f) Saisissez **yes** pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

FXOS décompresse l'ensemble et met à niveau/recharge les composants.

g) Pour surveiller le processus de mise à niveau, consultez Surveiller l'avancement de la mise à niveau, à la page 127.

Étape 5 Une fois que tous les composants ont bien été mis à niveau, vérifiez l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées avant de continuer (voir Vérifier l'installation, à la page 128).

Étape 6 Téléchargez la nouvelle image logicielle ASA sur le châssis :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Entrez le mode des logiciels d'application :

scope app-software

c) Téléchargez l'image logicielle du périphérique logique :

download image *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*nom_d_utilisateur@serveur*/*chemin*
- **scp**://*nom_d_utilisateur@serveur*/*chemin*
- **sftp**://*nom_d_utilisateur@serveur*/*chemin*
- **tftp**://*serveur*:*numéro_de_port*/*chemin*

d) Pour surveiller le processus de téléchargement :

show download-task

e) Pour afficher les applications téléchargées :

up

show app

Notez la version ASA pour le paquet que vous avez téléchargé. Vous devrez utiliser la chaîne de version exacte pour activer l'application à une étape ultérieure.

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Étape 7 Mettez à niveau l'image du périphérique logique ASA :

a) Entrez le mode de services de sécurité :

top

scope ssa

b) Définissez la portée au module de sécurité que vous mettez à jour :

scope slot*slot_number*

c) Définissez la portée de l'application ASA :

scope app-instance asa *instance_name*

d) Définissez la version de démarrage sur la version que vous souhaitez mettre à jour :

set startup-version *version_number*

e) Validez la configuration :

commit-buffer

Validez la transaction dans la configuration du système. L'image de l'application est mise à jour et l'application redémarre.

Étape 8 Pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées, consultez Vérifier l'installation, à la page 128.

Étape 9 Répétez les étapes Étape 2, à la page 124–Étape 8, à la page 127 pour tous les châssis restants de la grappe qui ne disposent pas de nœud de contrôle.

Étape 10 Une fois que tous les châssis de la grappe qui ne disposent pas de nœud de contrôle ont été mis à niveau, répétez les étapes Étape 2, à la page 124–Étape 8, à la page 127 sur le châssis **avec le nœud de contrôle**. Un nouveau nœud de contrôle sera choisi dans l'un des châssis précédemment mis à niveau.

Étape 11 Pour le mode de mise en grappe VPN distribuée, une fois que la grappe est stable, redistribuez les sessions actives entre tous les modules de la grappe à l'aide de la console ASA sur l'unité de contrôle.

cluster redistribute vpn-sessiondb

Prochaine étape

Définissez l'ID de site de châssis. Pour en savoir plus sur la définition de l'ID de site du châssis, consultez la rubrique sur la mise en grappe intersite dans Déploiement d'une grappe pour ASA sur le Firepower 4100/9300 pour l'évolutivité et la haute disponibilité sur Cisco.com.

Surveiller l'avancement de la mise à niveau

Vous pouvez surveiller le processus de mise à niveau à l'aide du Interface de ligne de commande FXOS :

Procédure

Étape 1 Connectez-vous au Interface de ligne de commande FXOS.

Étape 2 Entrez **scope system**.

Étape 3 Entrez **show firmware monitor**.

Étape 4 Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.

Remarque

Après la mise à niveau du composant FPRM, le système redémarrera puis poursuivra la mise à niveau des autres composants.

Exemple

```
Firepower-chassis# scope system
Firepower-chassis /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Vérifier l'installation

Saisissez les commandes suivantes pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées :

Procédure

Étape 1 Connectez-vous au Interface de ligne de commande FXOS.

Étape 2 Entrez **top**.

Étape 3 Entrez **scope ssa**.

Étape 4 Entrez **show slot**.

Étape 5 Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.

Exemple :

Étape 6 Entrez **show app-instance**.

Étape 7 Vérifiez que l'état d'exploitation est `en ligne` pour tous les périphériques logiques installés sur le châssis et que la bonne version est indiquée.

Si ce châssis fait partie d'une grappe, vérifiez que l'état opérationnel de la grappe est « In-Cluster » pour tous les modules de sécurité installés dans le châssis. Vérifiez également que l'unité de contrôle ne se trouve pas

sur le châssis pour lequel vous effectuez la mise à niveau : il ne doit y avoir aucune instance avec le rôle de grappe défini sur « Master ».

Exemple

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
Firepower-chassis /ssa #
Firepower-chassis /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 --------------- ------------
asa        asa1       1          Enabled     Online           9.10.0.85       9.10.0.85
    Not Applicable  None
asa        asa2       2          Enabled     Online           9.10.0.85       9.10.0.85
    Not Applicable  None
Firepower-chassis /ssa #
```

Mettre à niveau l'ASA Virtual, l'ISA 3000 ou l'ASA 5500-X

Ce document décrit comment planifier et mettre en œuvre une mise à niveau ASA et ASDM pour les déploiements autonomes, de basculement ou de mise en grappe sur les modèles suivants :

- ASA virtuel
- ISA 3000
- ASA 5500-X

Mettre à niveau une unité autonome

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau l'unité autonome.

Mettre à niveau une unité autonome à l'aide de l'interface de ligne de commande

Cette section décrit comment installer les images ASDM et ASA, et quand mettre à niveau le module ASA FirePOWER.

Avant de commencer

Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Procédure

Étape 1 En mode d'exécution privilégié, copiez le logiciel ASA dans la mémoire flash.

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa*
disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin
disk0:/asa-9-12-1-smp-k8.bin
```

Étape 2 Copiez l'image ASDM dans la mémoire flash.

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/asdm_image_name*
disk*n***:/**[*chemin/*]*asdm_image_name*

Exemple :

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

Étape 3 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Étape 4 Affichez les images de démarrage actuelles configurées (jusqu'à 4) :

show running-config boot system

L'ASA utilise les images dans l'ordre indiqué; si la première image n'est pas disponible, l'image suivante est utilisée, et ainsi de suite. Vous ne pouvez pas insérer une nouvelle URL d'image en haut de la liste. Pour placer la nouvelle image en première position, vous devez supprimer toutes les entrées existantes et saisir les URL d'image dans l'ordre souhaité, en fonction des étapes suivantes.

Exemple :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

Étape 5 Supprimez toutes les configurations d'image de démarrage existantes afin de pouvoir utiliser la nouvelle image de démarrage comme votre premier choix :

no boot system disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
```

```
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

Étape 6 Définissez l'image ASA à démarrer (celle que vous venez de charger) :

boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Répétez cette commande pour toutes les images de sauvegarde que vous souhaitez utiliser au cas où cette image ne serait pas disponible. Par exemple, vous pouvez réintroduire les images que vous avez précédemment supprimées.

Exemple :

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

Étape 7 Définissez l'image ASDM à utiliser (celle que vous venez de charger) :

asdm image disk*n***:/**[*chemin*/]*nom_de_l_image_asdm*

Vous ne pouvez configurer qu'une seule image ASDM à utiliser, vous n'avez donc pas besoin de supprimer la configuration existante en premier lieu.

Exemple :

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

Étape 8 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Étape 9 Rechargez l'ASA :

reload

Étape 10 Si vous mettez à niveau le module ASA FirePOWER, désactivez l'API REST ASA, sinon la mise à niveau échouera.

no rest-api agent

Vous pouvez la réactiver après la mise à niveau :

rest-api agent

Remarque
La série ASA 5506-X ne prend pas en charge l'API REST ASA si vous utilisez la version 6.0 du module FirePOWER ou une version ultérieure.

Étape 11 Mettez à niveau le module ASA FirePOWER.

Mettre à niveau une unité autonome à partir de votre ordinateur local à l'aide d'ASDM

L'**outil de mise à niveau du logiciel à partir de l'ordinateur local** vous permet de charger un fichier image de votre ordinateur vers le système de fichiers flash pour mettre à niveau l'ASA.

Procédure

Étape 1 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 2 Dans la liste déroulante **Image à charger**, sélectionnez **ASDM**.

Étape 3 Dans le champ **Chemin d'accès au fichier local**, cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 4 Dans le champ **Chemin d'accès au système de fichiers flash**, cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Étape 5 Cliquez sur **Charger une image**.

Le processus de chargement peut prendre quelques minutes.

Étape 6 Vous êtes invité à définir cette image comme image ASDM. Cliquez sur **Yes** (Oui).

Étape 7 Il vous est rappellé de quitter ASDM et d'enregistrer la configuration. Cliquez sur **OK**.

Vous quittez l'outil **Mise à niveau**. **Remarque :** Vous enregistrerez la configuration, puis quitterez et vous reconnecterez à ASDM *après* avoir mis à niveau le logiciel ASA.

Étape 8 Répétez ces étapes, en sélectionnant **ASA** dans la liste déroulante **Image à charger**. Vous pouvez également utiliser cette procédure pour charger d'autres types de fichiers.

Étape 9 Choisissez **Outils** > **Rechargement du système** pour recharger l'ASA.

Une nouvelle fenêtre s'affiche et vous demande de vérifier les détails du rechargement.

a) Cliquez sur le bouton radio **Enregistrer la configuration en cours d'enregistrement au moment du rechargement**.
b) Choisissez une heure de rechargement (par exemple, **Maintenant**, la valeur par défaut).
c) Cliquer sur **Planifier le rechargement**.

Une fois que le rechargement est en cours, une fenêtre **État du rechargement** s'affiche pour indiquer qu'un rechargement est en cours. Une option pour quitter ASDM est également fournie.

Étape 10 Après le rechargement de l'ASA, redémarrez ASDM.

Vous pouvez vérifier l'état de rechargement à partir d'un port de console, ou vous pouvez attendre quelques minutes et essayer de vous connecter à l'aide d'ASDM.

Étape 11 Si vous mettez à niveau un module ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande**et en entrant **no rest-api agent**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera. Vous pouvez la réactiver après la mise à niveau :

rest-api agent

Remarque
La série ASA 5506-X ne prend pas en charge l'API REST ASA si vous utilisez la version 6.0 du module FirePOWER ou une version ultérieure.

Étape 12 Mettez à niveau le module ASA FirePOWER.

Mettre à niveau une unité autonome à l'aide de l'assistant ASDM Cisco.com

L'**assistant de mise à niveau du logiciel à partir de Cisco.com** vous permet de mettre à niveau automatiquement ASDM et ASA vers des versions plus récentes.

Dans cet assistant, vous pouvez effectuer les opérations suivantes :

- Choisissez un fichier image ASA ou un fichier image ASDM à mettre à niveau.

Remarque ASDM télécharge la dernière version de l'image, qui comprend le numéro de version. Par exemple, si vous téléchargez la version 9.9(1), le téléchargement peut inclure la version 9.9(1.2). Ce comportement est normal, vous pouvez donc procéder à la mise à niveau prévue.

- Passez en revue les modifications de mise à niveau que vous avez apportées.
- Téléchargez l'image ou les images et installez-les.
- Passez en revue l'état de l'installation.
- Si l'installation a réussi, rechargez l'ASA pour enregistrer la configuration et terminer la mise à niveau.

Avant de commencer

En raison d'une modification interne, l'assistant est uniquement pris en charge par ASDM 7.10(1) ou les versions ultérieures. De plus, en raison d'une modification de nom d'image, vous devez utiliser ASDM 7.12(1) ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.10(1) ou une version ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM, quelle que soit la version d'ASA que vous utilisez.

Procédure

Étape 1 Choisissez **Outils** > **Vérifier la présence de mises à jour ASA/ASDM**.

En mode contexte multiple, accédez à ce menu à partir du système.

La boîte de dialogue **Authentification de Cisco.com** s'affiche.

Étape 2 Saisissez votre nom d'utilisateur et votre mot de passe Cisco.com, puis cliquez sur **Connexion**.

L'**assistant de mise à niveau Cisco.com** s'affiche.

Remarque
Si aucune mise à niveau n'est disponible, une boîte de dialogue s'affiche. Cliquez sur **OK** pour quitter l'assistant.

Étape 3 Cliquez sur **Suivant** pour afficher l'écran **Sélectionner un logiciel**.

La version d'ASA actuelle et la version d'ASDM s'affichent.

Étape 4 Pour mettre à niveau la version d'ASA et la version d'ASDM, procédez comme suit :

a) Dans la zone **ASA**, cochez la case **Mettre à niveau vers**, puis choisissez une version d'ASA à laquelle vous souhaitez passer dans la liste déroulante.

b) Dans la zone **ASDM**, cochez la case **Mettre à niveau vers**, puis choisissez une version d'ASDM à laquelle vous souhaitez passer dans la liste déroulante.

Étape 5 Cliquez sur **Suivant** pour afficher l'écran **Passer en revue les modifications**.

Étape 6 Vérifiez les éléments suivants :

- Le fichier image ASA ou le fichier image ASDM que vous avez téléchargé est le bon.
- Le fichier image ASA ou le fichier image ASDM que vous souhaitez charger est le bon.
- La bonne image de démarrage ASA a été sélectionnée.

Étape 7 Cliquez sur **Suivant** pour lancer l'installation de la mise à niveau.

Vous pouvez ensuite afficher l'état de l'installation de la mise à niveau à mesure qu'elle progresse.

L'écran **Résultats** s'affiche, et fournit des détails supplémentaires, comme l'état de l'installation de la mise à niveau (réussite ou échec).

Étape 8 Si l'installation de la mise à niveau a réussi, pour que les versions de mise à niveau prennent effet, cochez la case **Enregistrer la configuration et recharger le périphérique maintenant** pour redémarrer l'ASA et le redémarrer ASDM.

Étape 9 Cliquez sur **Terminer** pour quitter l'assistant et enregistrer les modifications de configuration que vous avez apportées.

Remarque
Pour passer à la version ultérieure, le cas échéant, vous devez redémarrer l'assistant.

Étape 10 Après le rechargement de l'ASA, redémarrez ASDM.

Vous pouvez vérifier l'état de rechargement à partir d'un port de console, ou vous pouvez attendre quelques minutes et essayer de vous connecter à l'aide d'ASDM.

Étape 11 Si vous mettez à niveau un module ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande**et en entrant **no rest-api agent**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera. Vous pouvez la réactiver après la mise à niveau :

rest-api agent

Remarque
La série ASA 5506-X ne prend pas en charge l'API REST ASA si vous utilisez la version 6.0 du module FirePOWER ou une version ultérieure.

Étape 12 Mettez à niveau le module ASA FirePOWER.

Mettre à niveau une paire de basculements actif/de secours

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau la paire de basculements actif/de secours pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une paire de basculements actif/de secours à l'aide de l'interface de ligne de commande

Pour mettre à niveau la paire de basculements actif/de secours, procédez comme suit.

Avant de commencer

- Exécutez ces étapes sur l'unité active. Pour l'accès SSH, connectez-vous à l'adresse IP active; l'unité active présente toujours cette adresse IP. Lorsque vous vous connectez à l'interface de ligne de commande, déterminez l'état de basculement en examinant l'invite d'ASA; vous pouvez configurer l'invite ASA pour afficher l'état et la priorité de basculement (principal ou secondaire), ce qui est utile pour déterminer à quelle unité vous êtes connecté. Consultez la commande d'invite. Vous pouvez également saisir la commande **show failover** pour afficher l'état et la priorité de cette unité (principale ou secondaire).
- Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Procédure

Étape 1 Sur l'unité active, en mode d'exécution privilégié, copiez le logiciel ASA dans la mémoire flash de l'unité active :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[/*chemin*]/*nom_de_l_image_asa*
disk*n***:**/[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

Étape 2 Copiez le logiciel sur l'unité de secours. Assurez-vous de définir le même chemin que pour l'unité active :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[/*chemin*]/*nom_de_l_image_asa* **disk***n***:**/[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

Étape 3 Copiez l'image ASDM dans la mémoire flash de l'unité active :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[/*chemin*]/*asdm_image_name*
disk*n***:**/[*chemin*/]*asdm_image_name*

Exemple :

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

Étape 4 Copiez l'image ASDM sur l'unité de secours. Assurez-vous de définir le même chemin que pour l'unité active :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/asdm_image_name* **disk***n***:/**[*chemin/*]*asdm_image_name*

Exemple :

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

Étape 5 Si vous n'êtes pas déjà en mode de configuration globale, accédez-y :

configure terminal

Étape 6 Affichez les images de démarrage actuelles configurées (jusqu'à 4) :

show running-config boot system

Exemple :

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

L'ASA utilise les images dans l'ordre indiqué; si la première image n'est pas disponible, l'image suivante est utilisée, et ainsi de suite. Vous ne pouvez pas insérer une nouvelle URL d'image en haut de la liste. Pour placer la nouvelle image en première position, vous devez supprimer toutes les entrées existantes et saisir les URL d'image dans l'ordre souhaité, en fonction des étapes suivantes.

Étape 7 Supprimez toutes les configurations d'image de démarrage existantes afin de pouvoir utiliser la nouvelle image de démarrage comme votre premier choix :

no boot system disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

Étape 8 Définissez l'image ASA à démarrer (celle que vous venez de charger) :

boot system disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

Répétez cette commande pour toutes les images de sauvegarde que vous souhaitez utiliser au cas où cette image ne serait pas disponible. Par exemple, vous pouvez réintroduire les images que vous avez précédemment supprimées.

Étape 9 Définissez l'image ASDM à utiliser (celle que vous venez de charger) :

asdm image disk*n***:/**[*chemin*/]*nom_de_l_image_asdm*

Exemple :

```
asa/act(config)# asdm image disk0:/asdm-77171417151.bin
```

Vous ne pouvez configurer qu'une seule image ASDM à utiliser, vous n'avez donc pas besoin de supprimer la configuration existante en premier lieu.

Étape 10 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Ces modifications de configuration sont automatiquement enregistrées sur l'unité de secours.

Étape 11 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA, sinon la mise à niveau échouera.

no rest-api agent

Étape 12 Mettez à niveau le module ASA FirePOWER sur l'unité de secours.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours*. Attendez que la mise à niveau soit terminée.

Étape 13 Rechargez l'unité de secours pour démarrer la nouvelle image :

failover reload-standby

Attendez que l'unité de secours ait terminé le chargement. Utilisez la commande **show failover** pour vérifier que l'unité de secours est à l'état de secours.

Étape 14 Forcez l'unité active à basculer vers l'unité de secours.

no failover active

Si vous êtes déconnecté de votre session SSH, reconnectez-vous à l'adresse IP principale, maintenant sur la nouvelle unité active/ancienne unité de secours.

Étape 15 Mettez à niveau le module ASA FirePOWER sur l'ancienne unité active.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours*. Attendez que la mise à niveau soit terminée.

Étape 16 À partir de la nouvelle unité active, rechargez l'ancienne unité active (maintenant la nouvelle unité de secours).

failover reload-standby

Exemple :

```
asa/act# failover reload-standby
```

Remarque
Si vous êtes connecté au port de console de l'ancienne unité active, vous devez plutôt saisir la commande **reload** pour recharger l'ancienne unité active.

Mettre à niveau une paire de basculements actif/de secours à l'aide d'ASDM

Pour mettre à niveau la paire de basculements actif/de secours, procédez comme suit.

Avant de commencer

Placez les images ASA et ASDM sur votre ordinateur de gestion local.

Procédure

Étape 1 Lancez ASDM sur l'unité *de secours* en vous connectant à l'adresse IP de secours.

Étape 2 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 3 Dans la liste déroulante **Image à charger**, sélectionnez **ASDM**.

Étape 4 Dans le champ **Chemin d'accès au fichier local**, saisissez le chemin d'accès local au fichier sur votre ordinateur ou cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 5 Dans le champ **Chemin d'accès au système de fichiers flash**, saisissez le chemin d'accès au système de fichiers flash ou cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Étape 6 Cliquez sur **Charger une image**. Le processus de chargement peut prendre quelques minutes.

Lorsque vous êtes invité à définir cette image comme image ASDM, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 7 Répétez ces étapes, en sélectionnant **ASA** dans la liste déroulante **Image à charger**.

Lorsque vous êtes invité à définir cette image comme image ASA, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 8 Connectez ASDM à l'unité *active* en vous connectant à l'adresse IP principale et chargez le logiciel ASDM en utilisant le même emplacement de fichier que vous avez utilisé sur l'unité de secours.

Étape 9 Lorsque vous êtes invité à définir l'image comme image ASDM, cliquez sur **Oui**.

Il vous est rappellé de quitter ASDM et d'enregistrer la configuration. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau. **Remarque :** Vous enregistrerez la configuration et rechargerez ASDM *après* avoir mis à niveau le logiciel ASA.

Étape 10 Chargez le logiciel ASA en utilisant le même emplacement de fichier que vous avez utilisé pour l'unité de secours.

Étape 11 Lorsque vous êtes invité à définir l'image comme image ASA, cliquez sur **Oui**.

Il vous est rappelé de recharger l'ASA pour utiliser la nouvelle image. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau.

Étape 12 Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Ces modifications de configuration sont automatiquement enregistrées sur l'unité de secours.

Étape 13 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande** et en saisissant **no rest-api enable**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera.

Étape 14 Mettez à niveau le module ASA FirePOWER sur l'unité de secours.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours*. Attendez que la mise à niveau soit terminée, puis reconnectez ASDM à l'unité active.

Étape 15 Rechargez l'unité de secours en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Recharger l'unité de secours**.

Restez dans le volet **Système** pour surveiller le rechargement de l'unité de secours.

Étape 16 Après le rechargement de l'unité de secours, forcez l'unité active à basculer vers l'unité de secours en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Faire passer en groupe de secours**.

ASDM se reconnectera automatiquement à la nouvelle unité active.

Étape 17 Mettez à niveau le module ASA FirePOWER sur l'ancienne unité active.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours*. Attendez que la mise à niveau soit terminée, puis reconnectez ASDM à l'unité active.

Étape 18 Rechargez l'unité de secours (nouvelle) en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Recharger l'unité de secours**.

Mettre à niveau une paire de basculements actif/actif

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau la paire de basculements actif/actif pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une paire de basculements actif/actif à l'aide de l'interface de ligne de commande

Pour mettre à niveau deux unités dans une configuration de basculement actif/actif, procédez comme suit.

Avant de commencer

- Exécutez ces étapes sur l'unité principale.
- Effectuez ces étapes dans l'espace d'exécution du système.
- Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Procédure

Étape 1 Sur l'unité principale, en mode d'exécution privilégié, copiez le logiciel ASA dans la mémoire flash :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa*
disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

Étape 2 Copiez le logiciel sur l'unité secondaire. Assurez-vous de définir le même chemin que pour l'unité principale :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

Étape 3 Copiez l'image ASDM dans la mémoire flash de l'unité principale :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/asdm_image_name*
disk*n***:/**[*chemin/*]*asdm_image_name*

Exemple :

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin
disk0:/asdm-77171417151.bin
```

Étape 4 Copiez l'image ASDM sur l'unité secondaire. Assurez-vous de définir le même chemin que pour l'unité principale :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/asdm_image_name*
disk*n***:/**[*chemin/*]*asdm_image_name*

Exemple :

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

Étape 5 Si vous n'êtes pas déjà en mode de configuration globale, accédez-y :

configure terminal

Étape 6 Affichez les images de démarrage actuelles configurées (jusqu'à 4) :

show running-config boot system

Exemple :

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

L'ASA utilise les images dans l'ordre indiqué; si la première image n'est pas disponible, l'image suivante est utilisée, et ainsi de suite. Vous ne pouvez pas insérer une nouvelle URL d'image en haut de la liste. Pour

placer la nouvelle image en première position, vous devez supprimer toutes les entrées existantes et saisir les URL d'image dans l'ordre souhaité, en fonction des étapes suivantes.

Étape 7 Supprimez toutes les configurations d'image de démarrage existantes afin de pouvoir utiliser la nouvelle image de démarrage comme votre premier choix :

no boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

Étape 8 Définissez l'image ASA à démarrer (celle que vous venez de charger) :

boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/act/pri(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

Répétez cette commande pour toutes les images de sauvegarde que vous souhaitez utiliser au cas où cette image ne serait pas disponible. Par exemple, vous pouvez réintroduire les images que vous avez précédemment supprimées.

Étape 9 Définissez l'image ASDM à utiliser (celle que vous venez de charger) :

asdm image disk*n***:/**[*chemin*/]*nom_de_l_image_asdm*

Exemple :

```
asa/act/pri(config)# asdm image disk0:/asdm-77171417151.bin
```

Vous ne pouvez configurer qu'une seule image ASDM à utiliser, vous n'avez donc pas besoin de supprimer la configuration existante en premier lieu.

Étape 10 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Ces modifications de configuration sont automatiquement enregistrées sur l'unité secondaire.

Étape 11 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA, sinon la mise à niveau échouera.

no rest-api agent

Étape 12 Activez les deux groupes de basculement sur l'unité principale :

failover active group 1

failover active group 2

Exemple :

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

Étape 13 Mettez à niveau le module ASA FirePOWER sur l'unité secondaire.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours* du groupe de basculement 1 ou 2. Attendez que la mise à niveau soit terminée.

Étape 14 Rechargez l'unité secondaire pour démarrer la nouvelle image :

failover reload-standby

Attendez que l'unité secondaire ait terminé le chargement. Utilisez la commande **show failover** pour vérifier que les deux groupes de basculement sont à l'état de secours.

Étape 15 Forcez les deux groupes de basculement à devenir actifs sur l'unité secondaire :

no failover active group 1

no failover active group 2

Exemple :

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

Si vous êtes déconnecté de votre session SSH, reconnectez-vous à l'adresse IP du groupe de basculement 1, maintenant sur l'unité secondaire.

Étape 16 Mettez à niveau le module ASA FirePOWER sur l'unité principale.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours* du groupe de basculement 1 ou 2. Attendez que la mise à niveau soit terminée.

Étape 17 Rechargez l'unité principale :

failover reload-standby

Exemple :

```
asa/act/sec# failover reload-standby
```

Remarque
Si vous êtes connecté au port de console de l'unité principale, vous devez plutôt saisir la commande **reload** pour recharger l'unité principale.

Il se peut que vous soyez déconnecté de votre session SSH.

Étape 18 Si les groupes de basculement sont configurés avec la commande **preempt**, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé.

Mettre à niveau une paire de basculements actif/actif à l'aide d'ASDM

Pour mettre à niveau deux unités dans une configuration de basculement actif/actif, procédez comme suit.

Avant de commencer

- Effectuez ces étapes dans l'espace d'exécution du système.

- Placez les images ASA et ASDM sur votre ordinateur de gestion local.

Procédure

Étape 1 Lancez ASDM sur l'unité *secondaire* en vous connectant à l'adresse de gestion dans le groupe de basculement 2.

Étape 2 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 3 Dans la liste déroulante **Image à charger**, sélectionnez **ASDM**.

Étape 4 Dans le champ **Chemin d'accès au fichier local**, saisissez le chemin d'accès local au fichier sur votre ordinateur ou cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 5 Dans le champ **Chemin d'accès au système de fichiers flash**, saisissez le chemin d'accès au système de fichiers flash ou cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Étape 6 Cliquez sur **Charger une image**. Le processus de chargement peut prendre quelques minutes.

Lorsque vous êtes invité à définir cette image comme image ASDM, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 7 Répétez ces étapes, en sélectionnant **ASA** dans la liste déroulante **Image à charger**.

Lorsque vous êtes invité à définir cette image comme image ASA, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 8 Connectez ASDM à l'unité *principale* en vous connectant à l'adresse IP de gestion dans le groupe de basculement 1 et chargez le logiciel ASDM en utilisant le même emplacement de fichier que vous avez utilisé sur l'unité secondaire.

Étape 9 Lorsque vous êtes invité à définir l'image comme image ASDM, cliquez sur **Oui**.

Il vous est rappellé de quitter ASDM et d'enregistrer la configuration. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau. **Remarque :** Vous enregistrerez la configuration et rechargerez ASDM *après* avoir mis à niveau le logiciel ASA.

Étape 10 Chargez le logiciel ASA en utilisant le même emplacement de fichier que vous avez utilisé pour l'unité secondaire.

Étape 11 Lorsque vous êtes invité à définir l'image comme image ASA, cliquez sur **Oui**.

Il vous est rappelé de recharger l'ASA pour utiliser la nouvelle image. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau.

Étape 12 Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Ces modifications de configuration sont automatiquement enregistrées sur l'unité secondaire.

Étape 13 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande** et en saisissant **no rest-api enable**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera.

Étape 14 Activez les deux groupes de basculement sur l'unité principale en sélectionnant **Surveillance** > **Basculement** > **Groupe de basculement #**, où **#** est le numéro du groupe de basculement que vous souhaitez déplacer dans l'unité principale, puis cliquez sur **Faire passer en groupe actif**.

Étape 15 Mettez à niveau le module ASA FirePOWER sur l'unité secondaire.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours* du groupe de basculement 1 ou 2. Attendez que la mise à niveau soit terminée, puis reconnectez ASDM à l'unité principale.

Étape 16 Rechargez l'unité secondaire en sélectionnant **Surveillance** > **Basculement** > **Système**, puis cliquez sur **Recharger l'unité de secours**.

Restez dans le volet **Système** pour surveiller le rechargement de l'unité secondaire.

Étape 17 Après le déploiement de l'unité secondaire, activez les deux groupes de basculement sur l'unité secondaire en sélectionnant **Surveillance** > **Basculement** > **Groupe de basculement #**, où **#** est le numéro du groupe de basculement que vous souhaitez déplacer dans l'unité secondaire, puis cliquez sur **Faire passer en groupe de secours**.

ASDM se reconnectera automatiquement à l'adresse IP du groupe de basculement 1 sur l'unité secondaire.

Étape 18 Mettez à niveau le module ASA FirePOWER sur l'unité principale.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours* du groupe de basculement 1 ou 2. Attendez que la mise à niveau soit terminée, puis reconnectez ASDM à l'unité secondaire.

Étape 19 Rechargez l'unité principale en sélectionnant **Surveillance** > **Basculement** > **Système**, puis cliquez sur **Recharger l'unité de secours**.

Étape 20 Si les groupes de basculement sont configurés avec la préemption activée, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé. ASDM se reconnectera automatiquement à l'adresse IP du groupe de basculement 1 sur l'unité principale.

Mettre à niveau une grappe ASA

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau la grappe ASA pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une grappe ASA à l'aide de l'interface de ligne de commande

Pour mettre à niveau toutes les unités d'une grappe ASA, suivez les étapes suivantes. Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Avant de commencer

- Exécutez ces étapes sur l'unité de contrôle. Si vous mettez également à niveau le module ASA FirePOWER, vous avez besoin d'un accès à la console ou à ASDM sur chaque unité de données. Vous pouvez configurer l'invite ASA pour afficher l'unité de la grappe et son état (contrôle ou données), ce qui est utile pour déterminer à quelle unité vous êtes connecté. Consultez la commande d'invite. Vous pouvez également saisir la commande **show cluster info** pour afficher le rôle de chaque unité.

- Vous devez utiliser le port de console; vous ne pouvez pas activer ni désactiver la mise en grappe à partir d'une connexion distante d'interface de ligne de commande.
- Effectuez ces étapes dans l'espace d'exécution du système pour le mode contexte multiple.

Procédure

Étape 1 Sur l'unité de contrôle en mode d'exécution privilégié, copiez le logiciel ASA sur toutes les unités de la grappe.

cluster exec copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

Étape 2 Copiez l'image ASDM sur toutes les unités de la grappe :

cluster exec copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/asdm_image_name* **disk***n***:/**[*chemin/*]*asdm_image_name*

Exemple :

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

Étape 3 Si vous n'êtes pas déjà en mode de configuration globale, accédez-y maintenant.

configure terminal

Exemple :

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

Étape 4 Affichez les images de démarrage actuelles configurées (jusqu'à 4).

show running-config boot system

Exemple :

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

L'ASA utilise les images dans l'ordre indiqué; si la première image n'est pas disponible, l'image suivante est utilisée, et ainsi de suite. Vous ne pouvez pas insérer une nouvelle URL d'image en haut de la liste. Pour placer la nouvelle image en première position, vous devez supprimer toutes les entrées existantes et saisir les URL d'image dans l'ordre souhaité, en fonction des étapes suivantes.

Étape 5 Supprimez toutes les configurations d'image de démarrage existantes afin de pouvoir utiliser la nouvelle image de démarrage comme votre premier choix :

no boot system disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

Étape 6 Définissez l'image ASA à démarrer (celle que vous venez de charger) :

boot system disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/unit1/master(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

Répétez cette commande pour toutes les images de sauvegarde que vous souhaitez utiliser au cas où cette image ne serait pas disponible. Par exemple, vous pouvez réintroduire les images que vous avez précédemment supprimées.

Étape 7 Définissez l'image ASDM à utiliser (celle que vous venez de charger) :

asdm image disk*n***:/**[*chemin/*]*nom_de_l_image_asdm*

Exemple :

```
asa/unit1/master(config)# asdm image disk0:/asdm-77171417151.bin
```

Vous ne pouvez configurer qu'une seule image ASDM à utiliser, vous n'avez donc pas besoin de supprimer la configuration existante en premier lieu.

Étape 8 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Ces modifications de configuration sont automatiquement enregistrées sur les unités de données.

Étape 9 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA, sinon la mise à niveau du module ASA FirePOWER échouera.

no rest-api agent

Étape 10 Si vous mettez à niveau des modules ASA FirePOWER gérés par ASDM, vous devrez connecter ASDM aux adresses IP de gestion *individuelles*, vous devez donc noter les adresses IP de chaque unité.

show running-config interface *ID_d_interface_de_gestion*

Notez le nom de regroupement **cluster-pool** utilisé.

show ip[**v6**] **local pool** *nom_de_regroupement*

Notez les adresses IP de l'unité de grappe.

Exemple :

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
```

```
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
unit1                           10.86.118.17
asa1/unit2/slave#
```

Étape 11 Mettez à niveau les unités de données.

Choisissez la procédure ci-dessous selon que vous mettez également à niveau des modules ASA FirePOWER. Les procédures ASA FirePOWER réduisent le nombre de rechargements de l'ASA lors de la mise à niveau du module ASA FirePOWER. Vous pouvez choisir d'utiliser la console de données ou ASDM pour ces procédures. Vous pouvez utiliser le module ASDM à la place de la console si vous n'avez pas accès à tous les ports de la console, mais que vous pouvez atteindre le module ASDM par le réseau.

Remarque
Pendant le processus de mise à niveau, n'utilisez jamais la commande **cluster master unit** pour forcer une unité de données à devenir l'unité de contrôle; vous pouvez causer des problèmes de connectivité au réseau et de stabilité de grappe. Vous devez d'abord mettre à niveau et recharger toutes les unités de données, puis poursuivre cette procédure pour assurer une transition harmonieuse de l'unité de contrôle actuelle vers une nouvelle unité de contrôle.

Si aucune mise à niveau du module ASA FirePOWER ne vous est proposée :

a) Sur l'unité de contrôle, pour afficher les noms de membre, saisissez **cluster exec unit ?**, ou saisissez la commande **show cluster info**.
b) Rechargez une unité de données.

cluster exec unit *unité_de_données* **reload noconfirm**

Exemple :

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) Répétez l'opération pour chaque unité de données.

Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, saisissez **show cluster info**.

Si une mise à niveau du module ASA FirePOWER vous est proposée (à l'aide de la console de données) :

a) Connectez-vous au port de console d'une unité de données et passez en mode de configuration globale.

enable

configure terminal

Exemple :

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) Désactivez la mise en grappe.

cluster group *name*

no enable

N'enregistrez pas cette configuration; vous voulez que la mise en grappe soit activée lorsque vous rechargez le nœud. Vous devez désactiver la mise en grappe pour éviter plusieurs défaillances et renouvellements pendant le processus de mise à niveau; cette unité ne doit se joindre qu'une fois la mise à niveau et le rechargement terminés.

Exemple :

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
either enable clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) Mettez à niveau le module ASA FirePOWER sur cette unité de données.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *individuelle* que vous avez notée plus tôt. Attendez que la mise à niveau soit terminée.

d) Rechargez l'unité de données.

reload noconfirm

e) Répétez l'opération pour chaque unité de données.

Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, saisissez **show cluster info**.

Si une mise à niveau du module ASA FirePOWER vous est proposée (à l'aide d'ASDM) :

a) Connectez ASDM à l'adresse IP de gestion *individuelle* de cette unité de données que vous avez notée plus tôt.

b) Choisissez **Configuration** > **Gestion des périphériques Haute disponibilité et évolutivité** > **Grappe ASA** > **Configuration de grappe** > **.**

c) Décochez la case **Participer à la grappe ASA**.

Vous devez désactiver la mise en grappe pour éviter plusieurs défaillances et renouvellements pendant le processus de mise à niveau; cette unité ne doit se joindre qu'une fois la mise à niveau et le rechargement terminés.

Ne décochez pas la case **Configurer les paramètres de grappe ASA**. Cette action efface toute la configuration de la grappe et désactive également toutes les interfaces, y compris l'interface de gestion

à laquelle ASDM est connecté. Pour rétablir la connectivité dans ce cas, vous devez accéder à l'interface de ligne de commande au niveau du port de console.

Remarque
Certaines anciennes versions d'ASDM ne prennent pas en charge la désactivation de la grappe sur cet écran; dans ce cas, utilisez l'outil **Outils** > **Interface de ligne de commande**, cliquez sur le bouton radio **Ligne multiple**, puis entrez **cluster group** *nom* et **no enable**. Vous pouvez afficher le nom du groupe de grappes dans la zone **Accueil** > **Tableau de bord des périphériques** > **Renseignements sur les périphériques** > **Grappe ASA**.

d) Cliquez sur **Apply**.
e) Vous êtes invité à quitter ASDM. Reconnectez ASDM à la même adresse IP.
f) Mettez à niveau le module ASA FirePOWER.

Attendez que la mise à niveau soit terminée.

g) Dans ASDM, choisissez **Outils** > **Rechargement du système**.
h) Cliquez sur le bouton radio **Recharger sans enregistrer la configuration en cours**.

Il ne faut pas sauvegarder la configuration. Lorsque cette unité sera rechargée, vous voudrez que la mise en grappe soit activée sur cette unité.

i) Cliquer sur **Planifier le rechargement**.
j) Cliquez sur **Oui** pour poursuivre le rechargement.
k) Répétez l'opération pour chaque unité de données.

Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, consultez le volet **Surveillance** > **Grappe ASA** > **Résumé de la grappe**de l'unité de contrôle.

Étape 12 Mettez à niveau l'unité de contrôle.

a) Désactivez la mise en grappe.

cluster group *name*

no enable

Attendez 5 minutes qu'une nouvelle unité de contrôle soit sélectionnée et que le trafic se stabilise.

N'enregistrez pas cette configuration; vous voulez que la mise en grappe soit activée lorsque vous rechargez le nœud.

Nous vous recommandons de désactiver manuellement la grappe sur l'unité de contrôle si possible afin qu'une nouvelle unité de contrôle puisse être choisie aussi rapidement et proprement que possible.

Exemple :

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
either enable clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) Mettez à niveau le module ASA FirePOWER sur cette unité.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *individuelle* que vous avez notée plus tôt. L'adresse IP de la grappe principale appartient maintenant à la nouvelle unité de contrôle. Cette ancienne unité de contrôle est toujours accessible sur son adresse IP de gestion individuelle.

Attendez que la mise à niveau soit terminée.

c) Rechargez cette unité.

reload noconfirm

Lorsque l'ancienne unité de contrôle rejoint la grappe, elle devient une unité de données.

Mettre à niveau une grappe ASA à l'aide d'ASDM

Pour mettre à niveau toutes les unités d'une grappe ASA, suivez les étapes suivantes.

Avant de commencer

- Exécutez ces étapes sur l'unité de contrôle. Si vous mettez également à niveau le module ASA FirePOWER, vous avez besoin d'un accès à ASDM sur chaque unité de données.
- Effectuez ces étapes dans l'espace d'exécution du système pour le mode contexte multiple.
- Placez les images ASA et ASDM sur votre ordinateur de gestion local.

Procédure

Étape 1 Lancez ASDM sur l'unité *de contrôle* en vous connectant à l'adresse IP principale de la grappe.

Cette adresse IP reste toujours avec l'unité de contrôle.

Étape 2 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel à partir de l'ordinateur local** s'affiche.

Étape 3 Cliquez sur le bouton radio **Tous les périphériques de la grappe**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 4 Dans la liste déroulante **Image à charger**, sélectionnez **ASDM**.

Étape 5 Dans le champ **Chemin d'accès au fichier local**, cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 6 (Facultatif) Dans le champ **Chemin d'accès au système de fichiers flash**, saisissez le chemin d'accès au système de fichiers flash ou cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Par défaut, ce champ est prérempli avec le chemin suivant : **disk0:/***filename*.

Étape 7 Cliquez sur **Charger une image**. Le processus de chargement peut prendre quelques minutes.

Étape 8 Vous êtes invité à définir cette image comme image ASDM. Cliquez sur **Yes** (Oui).

Étape 9 Il vous est rappellé de quitter ASDM et d'enregistrer la configuration. Cliquez sur **OK**.

Vous quittez l'outil Mise à niveau. **Remarque :** Vous enregistrerez la configuration et rechargerez ASDM *après* avoir mis à niveau le logiciel ASA.

Étape 10 Répétez ces étapes, en sélectionnant **ASA** dans la liste déroulante **Image à charger**.

Étape 11 Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Ces modifications de configuration sont automatiquement enregistrées sur les unités de données.

Étape 12 Notez les adresses IP de gestion individuelles pour chaque unité dans la section **Configuration** > **Gestion des périphériques** > **Haute disponibilité et évolutivité** > **Grappe ASA** > **Membres de la grappe** afin de pouvoir connecter ASDM directement aux unités de données ultérieurement.

Étape 13 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande** et en saisissant **no rest-api enable**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera.

Étape 14 Mettez à niveau les unités de données.

Choisissez la procédure ci-dessous selon que vous mettez également à niveau des modules ASA FirePOWER. La procédure ASA FirePOWER réduit le nombre de rechargements de l'ASA lors de la mise à niveau du module ASA FirePOWER.

Remarque
Pendant le processus de mise à niveau, ne modifiez jamais l'unité de contrôle à l'aide de la page **Surveillance** > **Grappe ASA** > **Résumé de la grappe** pour forcer une unité de données à devenir l'unité de contrôle; vous pouvez causer des problèmes de connectivité au réseau et de stabilité de grappe. Vous devez d'abord recharger toutes les unités de données, puis poursuivre cette procédure pour assurer une transition harmonieuse de l'unité de contrôle actuelle vers une nouvelle unité de contrôle.

Si aucune mise à niveau du module ASA FirePOWER ne vous est proposée :

a) Sur l'unité de contrôle, choisissez **Outils** > **Rechargement du système**.
b) Choisissez un nom d'unité de données dans la liste déroulante **Périphérique**.
c) Cliquer sur **Planifier le rechargement**.
d) Cliquez sur **Oui** pour poursuivre le rechargement.
e) Répétez l'opération pour chaque unité de données.

Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, consultez le volet **Surveillance** > **Grappe ASA** > **Résumé de la grappe**.

Si une mise à niveau du module ASA FirePOWER vous est proposée :

a) Sur l'unité de contrôle, choisissez la section **Configuration** > **Gestion des périphériques** > **Haute disponibilité et évolutivité** > **Grappe ASA** > **Membres de la grappe**.
b) Sélectionnez l'unité de données que vous souhaitez mettre à niveau, et cliquez sur **Supprimer**.
c) Cliquez sur **Apply**.
d) Quittez ASDM et connectez ASDM à l'unité de données en vous connectant à son adresse IP de gestion *individuelle* que vous avez notée plus tôt.

e) Mettez à niveau le module ASA FirePOWER.

Attendez que la mise à niveau soit terminée.

f) Dans ASDM, choisissez **Outils** > **Rechargement du système**.

g) Cliquez sur le bouton radio **Recharger sans enregistrer la configuration en cours**.

Il ne faut pas sauvegarder la configuration. Lorsque cette unité sera rechargée, vous voudrez que la mise en grappe soit activée sur cette unité.

h) Cliquer sur **Planifier le rechargement**.

i) Cliquez sur **Oui** pour poursuivre le rechargement.

j) Répétez l'opération pour chaque unité de données.

Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, consultez le volet **Surveillance** > **Grappe ASA** > **Résumé de la grappe**.

Étape 15 Mettez à niveau l'unité de contrôle.

a) Dans ASDM sur l'unité de contrôle, choisissez le volet **Configuration** > **Gestion des périphériques** > **Haute disponibilité et évolutivité** > **Grappe ASA** > **Configuration de grappe**.

b) Décochez la case **Participer à la grappe ASA**, puis cliquez sur **Appliquer**.

Vous êtes invité à quitter ASDM.

c) Attendez jusqu'à 5 minutes qu'une nouvelle unité de contrôle soit sélectionnée et que le trafic se stabilise.

Lorsque l'ancienne unité de contrôle rejoint la grappe, elle devient une unité de données.

d) Reconnectez ASDM à l'ancienne unité de contrôle en vous connectant à son adresse IP de gestion *individuelle* que vous avez notée plus tôt.

L'adresse IP de la grappe principale appartient maintenant à la nouvelle unité de contrôle. Cette ancienne unité de contrôle est toujours accessible sur son adresse IP de gestion individuelle.

e) Mettez à niveau le module ASA FirePOWER.

Attendez que la mise à niveau soit terminée.

f) Choisissez **Outils** > **Rechargement du système**.

g) Cliquez sur le bouton radio **Recharger sans enregistrer la configuration en cours**.

Il ne faut pas sauvegarder la configuration. Lorsque cette unité sera rechargée, vous voudrez que la mise en grappe soit activée sur cette unité.

h) Cliquer sur **Planifier le rechargement**.

i) Cliquez sur **Oui** pour poursuivre le rechargement.

Vous êtes invité à quitter ASDM. Redémarrez ASDM sur l'adresse IP de la grappe principale. Vous vous reconnecterez à la nouvelle unité de contrôle.

Mettre à niveau le Firepower 2100 en mode plateforme

Ce document décrit comment planifier et mettre en œuvre une mise à niveau ASA, FXOS et ASDM pour les déploiements autonomes ou de basculement pour le Firepower 2100 en mode plateforme. Avant la version 9.13, le Firepower 2100 prenait seulement en charge le mode plateforme. Dans les versions 9.14 et ultérieures, le mode appareil est le mode par défaut. Dans la version 9.14 et les versions ultérieures, utilisez la commande **show fxos mode** sur l'ASA pour déterminer votre mode actuel. Pour les procédures en mode appareil, consultez Mettre à niveau l'appareil ASA, à la page 75.

Mettre à niveau une unité autonome

Utilisez l'interface de ligne de commande de FXOS ou Firepower Chassis Manager pour mettre à niveau l'unité autonome.

Mettre à niveau une unité autonome à l'aide de Firepower Chassis Manager

Cette section décrit comment mettre à niveau l'offre groupée ASA, qui comprend ASA et ASDM, pour une unité autonome. Vous chargerez le paquet à partir de votre ordinateur de gestion.

Procédure

Étape 1 Si vous avez précédemment défini une image ASDM autre que celle par défaut dans la configuration ASA, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Dans la fenêtre principale de l'application ASDM, choisissez **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** (Configuration, Gestion de appareils, Image/Configuration du système, Image/Configuration de démarrage).
b) Pour le **chemin d'accès au fichier image ASDM**, saisissez **disk0:/asdm.bin**.
c) Cliquez sur **Appliquer**.
d) Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.
e) Quittez ASDM.

Étape 2 Connectez-vous au Firepower Chassis Manager.

Étape 3 Sélectionnez **System** > **Updates**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.

Étape 4 Cliquez sur **Charger l'image** pour charger le nouveau paquet à partir de votre ordinateur de gestion.

Étape 5 Cliquez sur **Choisir un fichier** pour accéder au paquet à charger et le sélectionner.

Étape 6 Cliquez sur **Charger**.

Le paquet sélectionné est chargé sur le châssis. La boîte de dialogue **Charger l'image** affiche l'état du chargement. Attendez que la boîte de dialogue **Réussite** s'affiche, puis cliquez sur **OK**. Une fois que le chargement est terminé, l'intégrité de l'image est automatiquement vérifiée.

Étape 7 Cliquez sur l'icône **Mise à niveau** à droite du nouveau paquet.

Étape 8 Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

Il n'y a aucun indicateur que le nouveau paquet est en cours de chargement. Vous verrez toujours le Firepower Chassis Manager au début du processus de mise à niveau. Lorsque le système redémarrera, vous serez déconnecté. Vous devez attendre que le système redémarre avant de pouvoir vous connecter au Firepower Chassis Manager. Le processus de redémarrage prend environ 20 minutes. Après le redémarrage, vous verrez l'écran de connexion.

Mettre à niveau une unité autonome à l'aide de l'interface de ligne de commande de FXOS

Cette section décrit comment mettre à niveau l'offre groupée ASA, qui comprend ASA et ASDM, pour une unité autonome. Vous pouvez utiliser le protocole FTP, SCP, SFTP ou TFTP pour copier le paquet sur le châssis Firepower 2100.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de FXOS, à partir du port de console (méthode préférée) ou à l'aide du protocole SSH.

Étape 2 Si vous avez précédemment défini une image ASDM autre que celle par défaut dans la configuration ASA, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Connectez-vous à ASA.

connect asa

Exemple :

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

b) Accédez au mode d'exécution privilégié, puis au mode de configuration globale.

enable

configure terminal

c) Définissez l'image ASDM.

asdm image disk0:/asdm.bin

d) Enregistrez la configuration.

write memory

e) Revenez à la console FXOS en entrant **Ctrl+a**, **d**.

Étape 3 Dans FXOS, téléchargez le paquet sur le châssis.

a) Entrez en mode micrologiciel.

scope firmware

Exemple :

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) Téléchargez le paquet.

download image *url*

Précisez l'URL du fichier en cours d'importation en utilisant l'un des modèles suivants :

- **ftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **scp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **sftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **tftp:**//*serveur*[**:***port*]/[*chemin_d_accès*/]*nom_de_l_image*

Exemple :

```
firepower-2110 /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Surveillez le processus de téléchargement.

show download-task

Exemple :

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181            0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181            0                 Downloading
firepower-2110 /firmware #
```

Étape 4 Lorsque le nouveau paquet termine le téléchargement (état **Téléchargé**), lancez le paquet.

a) Affichez le numéro de version du nouveau paquet.

show package

Exemple :

```
firepower-2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
firepower-2110 /firmware #
```

b) Installez le paquet.

scope auto-install

install security-pack version *version*

Dans la sortie **show package** , copiez la valeur **Paquet-Vers** pour le numéro **security-pack version**. Le châssis installe l'image ASA et redémarre.

Exemple :

```
firepower-2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

Étape 5 Attendez que le châssis ait terminé de redémarrer (de 5 à 10 minutes).

Bien que FXOS soit activé, vous devez toujours attendre que l'ASA s'affiche (5 minutes). Attendez que les messages suivants s'affichent :

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
```

[…]

Mettre à niveau une paire de basculements actif/de secours

Utilisez l'interface de ligne de commande de FXOS ou Firepower Chassis Manager pour mettre à niveau la paire de basculements actif/de secours pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une paire de basculements actif/de secours à l'aide de Firepower Chassis Manager

Cette section décrit comment mettre à niveau l'offre groupée ASA, qui comprend ASA et ASDM, pour une paire de basculements actif/de secours. Vous chargerez le paquet à partir de votre ordinateur de gestion.

Avant de commencer

Vous devez déterminer quelle unité est active et laquelle est considérée comme étant de secours : connectez ASDM à l'adresse IP ASA active. L'unité active est toujours propriétaire de l'adresse IP active. Ensuite, sélectionnez **Surveillance** > **Propriétés** > **Basculement** > **État** pour afficher la priorité de cette unité (principale ou secondaire) afin de savoir à quelle unité vous êtes connecté.

Procédure

Étape 1 Si vous avez précédemment défini une image ASDM autre que celle par défaut dans la configuration ASA, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Connectez-vous à ASDM sur l'unité *active*.
b) Dans la fenêtre principale de l'application ASDM, choisissez **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** (Configuration, Gestion de appareils, Image/Configuration du système, Image/Configuration de démarrage).
c) Pour le **chemin d'accès au fichier image ASDM**, saisissez **disk0:/asdm.bin**.
d) Cliquez sur **Appliquer**.
e) Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.
f) Quittez ASDM.

Étape 2 Mettez à niveau l'unité *de secours*.

a) Connectez-vous au Firepower Chassis Manager sur l'unité *de secours*.
b) Choisissez **Système** > **Mises à jour**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.
c) Cliquez sur **Charger l'image** pour charger le nouveau paquet à partir de votre ordinateur de gestion.
d) Cliquez sur **Choisir un fichier** pour accéder au paquet à charger et le sélectionner.

e) Cliquez sur **Charger**.

Le paquet sélectionné est chargé sur le châssis. La boîte de dialogue **Charger l'image** affiche l'état du chargement. Attendez que la boîte de dialogue **Réussite** s'affiche, puis cliquez sur **OK**. Une fois que le chargement est terminé, l'intégrité de l'image est automatiquement vérifiée.

f) Cliquez sur l'icône **Mise à niveau** à droite du nouveau paquet.

g) Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

Il n'y a aucun indicateur que le nouveau paquet est en cours de chargement. Vous verrez toujours le Firepower Chassis Manager au début du processus de mise à niveau. Lorsque le système redémarrera, vous serez déconnecté. Vous devez attendre que le système redémarre avant de pouvoir vous connecter au Firepower Chassis Manager. Le processus de redémarrage prend environ 20 minutes. Après le redémarrage, vous verrez l'écran de connexion.

Étape 3 Faites de l'unité que vous venez de mettre à niveau l'unité active afin que le trafic flux de trafic vers l'unité mise à niveau.

a) Lancez ASDM sur l'unité *de secours* en vous connectant à l'adresse IP de l'ASA de secours.

b) Forcez l'unité de secours à devenir active en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Faire passer en groupe actif**.

Étape 4 Mettez à niveau l'ancienne unité *active*.

a) Connectez-vous au Firepower Chassis Manager sur l'ancienne unité *active*.

b) Choisissez **Système** > **Mises à jour**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.

c) Cliquez sur **Charger l'image** pour charger le nouveau paquet à partir de votre ordinateur de gestion.

d) Cliquez sur **Choisir un fichier** pour accéder au paquet à charger et le sélectionner.

e) Cliquez sur **Charger**.

Le paquet sélectionné est chargé sur le châssis. La boîte de dialogue **Charger l'image** affiche l'état du chargement. Attendez que la boîte de dialogue **Réussite** s'affiche, puis cliquez sur **OK**. Une fois que le chargement est terminé, l'intégrité de l'image est automatiquement vérifiée.

f) Cliquez sur l'icône **Mise à niveau** à droite du nouveau paquet.

g) Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

Il n'y a aucun indicateur que le nouveau paquet est en cours de chargement. Vous verrez toujours le Firepower Chassis Manager au début du processus de mise à niveau. Lorsque le système redémarrera, vous serez déconnecté. Vous devez attendre que le système redémarre avant de pouvoir vous connecter au Firepower Chassis Manager. Le processus de redémarrage prend environ 20 minutes. Après le redémarrage, vous verrez l'écran de connexion.

Mettre à niveau une paire de basculements actif/de secours à l'aide de l'interface de ligne de commande de FXOS

Cette section décrit comment mettre à niveau l'offre groupée ASA, qui comprend ASA et ASDM, pour une paire de basculements actif/de secours. Vous pouvez utiliser le protocole FTP, SCP, SFTP ou TFTP pour copier le paquet sur le châssis Firepower 2100.

Avant de commencer

Vous devez déterminer quelle unité est active et laquelle est considérée comme étant de secours. Pour déterminer l'état de basculement, examinez l'invite d'ASA; vous pouvez configurer l'invite ASA pour afficher l'état et la priorité de basculement (principal ou secondaire), ce qui est utile pour déterminer à quelle unité vous êtes connecté. Consultez la commande d'invite. Cependant, l'invite FXOS n'est pas au courant du basculement de l'ASA. Vous pouvez également saisir la commande ASA **show failover** pour afficher l'état et la priorité de cette unité (principale ou secondaire).

Procédure

Étape 1 Si vous avez précédemment défini une image ASDM autre que celle par défaut dans la configuration ASA, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Connectez-vous à l'interface de ligne de commande de FXOS sur l'unité *active*, à partir du port de console (méthode préférée) ou à l'aide du protocole SSH.

b) Connectez-vous à ASA.

connect asa

Exemple :

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

c) Accédez au mode d'exécution privilégié, puis au mode de configuration globale.

enable

configure terminal

d) Définissez l'image ASDM.

asdm image disk0:/asdm.bin

e) Enregistrez la configuration.

write memory

f) Revenez à la console FXOS en entrant **Ctrl+a**, **d**.

Étape 2 Mettez à niveau l'unité *de secours*.

a) Connectez-vous à l'interface de ligne de commande de FXOS sur l'unité *de secours*, à partir du port de console (méthode préférée) ou à l'aide du protocole SSH.

b) Entrez en mode micrologiciel.

scope firmware

Exemple :

```
2110-sec# scope firmware
2110-sec /firmware#
```

c) Téléchargez le paquet.

download image *url*

Précisez l'URL du fichier en cours d'importation en utilisant l'un des modèles suivants :

- **ftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **scp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **sftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **tftp:**//*serveur*[**:***port*]/[*chemin_d_accès*/]*nom_de_l_image*

Exemple :

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

d) Surveillez le processus de téléchargement.

show download-task

Exemple :

```
2110-sec /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-sec /firmware #
```

e) Lorsque le nouveau paquet termine le téléchargement (état **Téléchargé**), lancez le paquet. Affichez le numéro de version du nouveau paquet.

show package

Exemple :

```
2110-sec /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-sec /firmware #
```

f) Installez le paquet.

scope auto-install

install security-pack version *version*

Dans la sortie **show package** , copiez la valeur **Paquet-Vers** pour le numéro **security-pack version**. Le châssis installe l'image ASA et redémarre.

Exemple :

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

g) Attendez que le châssis ait terminé de redémarrer (de 5 à 10 minutes).

Bien que FXOS soit activé, vous devez toujours attendre que l'ASA s'affiche (5 minutes). Attendez que les messages suivants s'affichent :

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

Étape 3 Faites de l'unité que vous venez de mettre à niveau l'unité active afin que le trafic flux de trafic vers l'unité mise à niveau.

a) Connectez-vous à l'interface de ligne de commande ASA de secours à partir de FXOS.

connect asa

enable

Exemple :

```
2110-sec# connect asa
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/stby/sec> enable
Password: *****
asa/stby/sec#
```

b) Forcez l'unité de secours à devenir active.

failover active

Exemple :

```
asa/stby/sec> failover active
asa/act/sec#
```

c) Pour revenir à la console FXOS, entrez **Ctrl+a**, **d**.

Étape 4 Mettez à niveau l'ancienne unité *active*.

a) Connectez-vous à l'interface de ligne de commande de FXOS sur l'ancienne unité *active*, à partir du port de console (méthode préférée) ou à l'aide du protocole SSH.

b) Entrez en mode micrologiciel.

scope firmware

Exemple :

```
2110-pri# scope firmware
2110-pri /firmware#
```

c) Téléchargez le paquet.

download image *url*

Précisez l'URL du fichier en cours d'importation en utilisant l'un des modèles suivants :

- **ftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **scp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **sftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **tftp:**//*serveur*[**:***port*]/[*chemin_d_accès*/]*nom_de_l_image*

Exemple :

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

d) Surveillez le processus de téléchargement.

show download-task

Exemple :

```
2110-pri /firmware # show download

Download task:
```

```
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-pri /firmware #
```

e) Lorsque le nouveau paquet termine le téléchargement (état **Téléchargé**), lancez le paquet. Affichez le numéro de version du nouveau paquet.

show package

Exemple :

```
2110-pri /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-pri /firmware #
```

f) Installez le paquet.

scope auto-install

install security-pack version *version*

Dans la sortie **show package** , copiez la valeur **Paquet-Vers** pour le numéro **security-pack version**. Le châssis installe l'image ASA et redémarre.

Exemple :

```
2110-pri /firmware # scope auto-install
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #
```

g) Attendez que le châssis ait terminé de redémarrer (de 5 à 10 minutes).

Bien que FXOS soit activé, vous devez toujours attendre que l'ASA s'affiche (5 minutes). Attendez que les messages suivants s'affichent :

```
2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

Mettre à niveau une paire de basculements actif/actif

Utilisez l'interface de ligne de commande de FXOS ou Firepower Chassis Manager pour mettre à niveau la paire de basculements actif/actif pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une paire de basculements actif/actif à l'aide de Firepower Chassis Manager

Cette section décrit comment mettre à niveau l'offre groupée ASA, qui comprend ASA et ASDM, pour une paire de basculements actif/actif. Vous chargerez le paquet à partir de votre ordinateur de gestion.

Procédure

Étape 1 Activez les deux groupes de basculement sur l'unité *principale*.

a) Lancez ASDM sur l'unité *principale* (ou l'unité avec le groupe de basculement 1 actif) en vous connectant à l'adresse de gestion dans le groupe de basculement 1.
b) Choisissez **Surveillance** > **Basculement** > **Groupe de basculement 2**, puis cliquez sur **Faire passer en groupe actif**.
c) Restez connecté à ASDM sur cette unité pour les étapes ultérieures.

Étape 2 Si vous avez précédemment défini une image ASDM autre que celle par défaut dans la configuration ASA, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Dans la fenêtre principale de l'application ASDM sur l'unité principale, choisissez **Configuration** > **Gestion des périphériques** > **Image du système/Configuration** > **Image de démarrage/Configuration**.
b) Pour le **chemin d'accès au fichier image ASDM**, saisissez **disk0:/asdm.bin**.
c) Cliquez sur **Appliquer**.

d) Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Étape 3 Mettez à niveau l'unité *secondaire*.

a) Connectez-vous au Firepower Chassis Manager sur l'unité *secondaire*.
b) Sélectionnez **System** > **Updates**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.
c) Cliquez sur **Charger l'image** pour charger le nouveau paquet à partir de votre ordinateur de gestion.
d) Cliquez sur **Choisir un fichier** pour accéder au paquet à charger et le sélectionner.
e) Cliquez sur **Charger**.

Le paquet sélectionné est chargé sur le châssis. La boîte de dialogue **Charger l'image** affiche l'état du chargement. Attendez que la boîte de dialogue **Réussite** s'affiche, puis cliquez sur **OK**. Une fois que le chargement est terminé, l'intégrité de l'image est automatiquement vérifiée.

f) Cliquez sur l'icône **Mise à niveau** à droite du nouveau paquet.
g) Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

Il n'y a aucun indicateur que le nouveau paquet est en cours de chargement. Vous verrez toujours le Firepower Chassis Manager au début du processus de mise à niveau. Lorsque le système redémarrera, vous serez déconnecté. Vous devez attendre que le système redémarre avant de pouvoir vous connecter au Firepower Chassis Manager. Le processus de redémarrage prend environ 20 minutes. Après le redémarrage, vous verrez l'écran de connexion.

Étape 4 Activez les deux groupes de basculement sur l'unité secondaire. Dans ASDM sur l'unité *principale*, choisissez **Surveillance** > **Basculement** > **Groupe de basculement 1**, puis cliquez sur **Faire passer en groupe de secours**.

ASDM se reconnectera automatiquement à l'adresse IP du groupe de basculement 1 sur l'unité secondaire.

Étape 5 Mettez à niveau l'unité *principale*.

a) Connectez-vous au Firepower Chassis Manager sur l'unité *principale*.
b) Sélectionnez **System** > **Updates**.
La zone **Mises à jour disponibles** affiche une liste des paquets disponibles sur le châssis.
c) Cliquez sur **Charger l'image** pour charger le nouveau paquet à partir de votre ordinateur de gestion.
d) Cliquez sur **Choisir un fichier** pour accéder au paquet à charger et le sélectionner.
e) Cliquez sur **Charger**.

Le paquet sélectionné est chargé sur le châssis. La boîte de dialogue **Charger l'image** affiche l'état du chargement. Attendez que la boîte de dialogue **Réussite** s'affiche, puis cliquez sur **OK**. Une fois que le chargement est terminé, l'intégrité de l'image est automatiquement vérifiée.

f) Cliquez sur l'icône **Mise à niveau** à droite du nouveau paquet.
g) Cliquez sur **Oui** pour confirmer que vous souhaitez poursuivre l'installation.

Il n'y a aucun indicateur que le nouveau paquet est en cours de chargement. Vous verrez toujours le Firepower Chassis Manager au début du processus de mise à niveau. Lorsque le système redémarrera, vous serez déconnecté. Vous devez attendre que le système redémarre avant de pouvoir vous connecter au Firepower Chassis Manager. Le processus de redémarrage prend environ 20 minutes. Après le redémarrage, vous verrez l'écran de connexion.

Étape 6 Si les groupes de basculement sont configurés avec la préemption activée, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé. Si les groupes de basculement ne sont pas

configurés avec la préemption activée, vous pouvez les rétablir à l'état actif sur leurs unités désignées à l'aide du volet ASDM **Surveillance > Basculement > Groupe de basculement #**.

Mettre à niveau une paire de basculements actif/actif à l'aide de l'interface de ligne de commande de FXOS

Cette section décrit comment mettre à niveau l'offre groupée ASA, qui comprend ASA et ASDM, pour une paire de basculements actif/actif. Vous pouvez utiliser le protocole FTP, SCP, SFTP ou TFTP pour copier le paquet sur le châssis Firepower 2100.

Procédure

Étape 1 Si vous avez précédemment défini une image ASDM autre que celle par défaut dans la configuration ASA, réinitialisez-la à l'image fournie avec votre ensemble d'images.

L'ensemble d'images inclut l'image ASDM, et 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 après le rechargement, car elles portent le même nom (**asdm.bin**). Si vous avez choisi manuellement une autre image ASDM que vous avez chargée (par exemple, **asdm-7191.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'utiliser une version compatible d'ASDM, vous devez reconfigurer l'ASA de manière à utiliser l'image ASDM fournie.

a) Connectez-vous à l'interface de ligne de commande de FXOS sur l'unité *principale*, à partir du port de console (méthode préférée) ou à l'aide du protocole SSH.

b) Connectez-vous à ASA.

connect asa

Exemple :

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

c) Accédez au mode d'exécution privilégié, puis au mode de configuration globale.

enable

configure terminal

d) Définissez l'image ASDM.

asdm image disk0:/asdm.bin

e) Enregistrez la configuration.

write memory

f) Revenez à la console FXOS en entrant **Ctrl+a**, **d**.

Étape 2 Connectez-vous à l'interface de ligne de commande de FXOS sur l'unité *secondaire*, à partir du port de console (méthode préférée) ou à l'aide du protocole SSH.

Étape 3 Activez les deux groupes de basculement sur l'unité principale.

a) Connectez-vous à l'interface de ligne de commande d'ASA à partir de FXOS.

connect asa

enable

Le mot de passe d'activation est vide par défaut.

Exemple :

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/act/sec> enable
Password: <blank>
asa/act/sec#
```

b) Activez les deux groupes de basculement sur l'unité principale.

no failover active group 1

no failover active group 2

Exemple :

```
asa/act/sec# no failover active group 1
asa/act/sec# no failover active group 2
```

c) Pour revenir à la console FXOS, entrez **Ctrl+a**, **d**.

Étape 4 Mettez à niveau l'unité *secondaire*.

a) Dans FXOS, passez en mode micrologiciel.

scope firmware

Exemple :

```
2110-sec# scope firmware
2110-sec /firmware#
```

b) Téléchargez le paquet.

download image *url*

Précisez l'URL du fichier en cours d'importation en utilisant l'un des modèles suivants :

- **ftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **scp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **sftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **tftp:**//*serveur*[**:***port*]/[*chemin_d_accès*/]*nom_de_l_image*

Exemple :

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Surveillez le processus de téléchargement.

show download-task

Exemple :

```
2110-sec /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-sec /firmware #
```

d) Lorsque le nouveau paquet termine le téléchargement (état **Téléchargé**), lancez le paquet. Affichez le numéro de version du nouveau paquet.

show package

Exemple :

```
2110-sec /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-sec /firmware #
```

e) Installez le paquet.

scope auto-install

install security-pack version *version*

Dans la sortie **show package** , copiez la valeur **Paquet-Vers** pour le numéro **security-pack version**. Le châssis installe l'image ASA et redémarre.

Exemple :

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes
```

```
Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

f) Attendez que le châssis ait terminé de redémarrer (de 5 à 10 minutes).

Bien que FXOS soit activé, vous devez toujours attendre que l'ASA s'affiche (5 minutes). Attendez que les messages suivants s'affichent :

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

Étape 5 Activez les deux groupes de basculement sur l'unité secondaire.

a) Connectez-vous à l'interface de ligne de commande d'ASA à partir de FXOS.

connect asa

enable

Le mot de passe d'activation est vide par défaut.

Exemple :

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/stby/sec> enable
Password: <blank>
asa/stby/sec#
```

b) Activez les deux groupes de basculement sur l'unité secondaire.

failover active group 1

failover active group 2

Exemple :

```
asa/stby/sec# failover active group 1
asa/act/sec# failover active group 2
```

c) Pour revenir à la console FXOS, entrez **Ctrl+a**, **d**.

Étape 6 Mettez à niveau l'unité *principale*.

a) Connectez-vous à l'interface de ligne de commande de FXOS sur l'unité *principale*, à partir du port de console (méthode préférée) ou à l'aide du protocole SSH.

b) Entrez en mode micrologiciel.

scope firmware

Exemple :

```
2110-pri# scope firmware
2110-pri /firmware#
```

c) Téléchargez le paquet.

download image *url*

Précisez l'URL du fichier en cours d'importation en utilisant l'un des modèles suivants :

- **ftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **scp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **sftp:**//*nom_d_utilisateur@serveur*/[*chemin_d_accès*/]*nom_de_l_image*
- **tftp:**//*serveur*[**:***port*]/[*chemin_d_accès*/]*nom_de_l_image*

Exemple :

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

d) Surveillez le processus de téléchargement.

show download-task

Exemple :

```
2110-pri /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-pri /firmware #
```

e) Lorsque le nouveau paquet termine le téléchargement (état **Téléchargé**), lancez le paquet. Affichez le numéro de version du nouveau paquet.

show package

Exemple :

```
2110-pri /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-pri /firmware #
```

f) Installez le paquet.

scope auto-install

install security-pack version *version*

Dans la sortie **show package** , copiez la valeur **Paquet-Vers** pour le numéro **security-pack version**. Le châssis installe l'image ASA et redémarre.

Exemple :

```
2110-pri /firmware # scope auto-install
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #
```

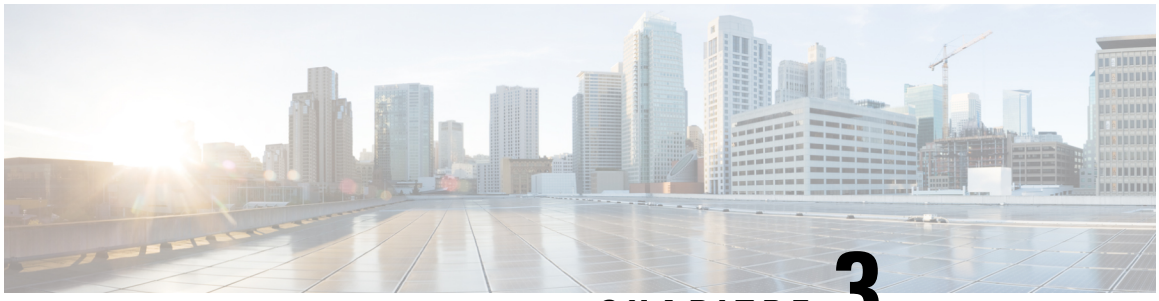
g) Attendez que le châssis ait terminé de redémarrer (de 5 à 10 minutes).

Bien que FXOS soit activé, vous devez toujours attendre que l'ASA s'affiche (5 minutes). Attendez que les messages suivants s'affichent :

```
2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

Étape 7 Si les groupes de basculement sont configurés avec la commande ASA **preempt**, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé. Si les groupes de basculement ne sont pas configurés avec la commande **preempt**, vous pouvez les rétablir à l'état actif sur leurs unités désignées en vous connectant à l'interface de ligne de commande d'ASA et en vous servant de la commande **failover active group**.



CHAPITRE 3

Rétrograder l'ASA

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, à la page 173
- Configuration incompatible supprimée après la rétrogradation, à la page 175
- Rétrograder l'appareil ASA, à la page 176
- Rétrograder le Firepower 2100 en mode plateforme, à la page 177
- Rétrograder le Firepower 4100/9300, à la page 177
- Rétrograder l'ISA 3000 ou l'ASA 5500-X , à la page 178

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 9.22 ou de toute version ultérieure** : si vous désactivez le port USB à l'aide de la commande USB-port disable, mais que vous le rétrogradez à une version antérieure, le port restera désactivé et vous ne pourrez pas le réactiver sans effacer la NVRAM (la commande **erase secure all** de la gestion locale FXOS).
- **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 > Gestion des périphériques > Licence > Licences Smart** et utilisez l'option **Forcer l'enregistrement**) et obtenir 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 Directives et migrations propres à la version, à la page 1 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 173.

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 Mettre à niveau l'appareil ASA, à la page 75 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 **Outils** > **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 gestionnaire de châssis 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 Mettre à niveau le Firepower 2100 en mode plateforme, à la page 153 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 gestionnaire de châssis 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 Mettre à niveau le Firepower 4100/9300, à la page 94 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 gestionnaire de châssis 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 Mettre à niveau le Firepower 4100/9300, à la page 94 pour les déploiements autonomes, de basculement ou de mise en grappe.

Rétrograder l'ISA 3000 ou l'ASA 5500-X

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

- Effacement de la configuration de l'image de démarrage (**clear configure boot**).
- Définition de l'image de démarrage comme étant l'ancienne image (**boot system**).
- (Facultatif) Entrée d'une nouvelle clé d'activation (**activation-key**).

- Enregistrement de la configuration en cours pour le démarrage (**write memory**). Cette opération définit la variable d'environnement BOOT sur l'ancienne image, de sorte que lorsque vous rechargez, l'ancienne image est chargée.
- Copie de l'ancienne sauvegarde de configuration dans la configuration de démarrage (**copy** *ancienne_url_de_configuration* **startup-config**).
- Rechargement (**reload**).

Avant de commencer

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

Procédure

Étape 1 **Interface de ligne de commande d'ASA :** 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.

Étape 2 **ASDM :** choisissez **Outils** > **Rétrograder le logiciel**.

La boîte de dialogue Rétrograder le logiciel s'affiche.

Étape 3 Pour l'**image ASA**, cliquez sur **Sélectionner un fichier d'image**.

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

Étape 4 Cliquez sur l'un des boutons radio suivants :

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

Étape 5 Pour la **configuration**, cliquez sur **Parcourir la mémoire flash** pour choisir le fichier de configuration de pré-migration.

Étape 6 (Facultatif) Dans le champ **Clé d'activation**, saisissez l'ancienne clé d'activation si vous devez rétablir une clé d'activation antérieure à la version 8.3.

Étape 7 Cliquez sur **Rétrograder**.

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.