

Accès de gestion

Ce chapitre décrit comment accéder à l'ASA pour la gestion de systèmes par le biais de Telnet, SSH et HTTPS (à l'aide d'ASDM), authentifier et autoriser les utilisateurs, et créer des bannières de connexion.

- Configurer l'accès de gestion à distance, à la page 1
- Configurer AAA pour les administrateurs système, à la page 21
- Accès au moniteur, à la page 39
- Historique de l'accès de gestion, à la page 39

Configurer l'accès de gestion à distance

Cette section décrit comment configurer l'accès ASA pour ASDM, Telnet ou SSH, et d'autres paramètres de gestion tels qu'une bannière de connexion.

Configurer l'accès ASA pour HTTPS, Telnet ou SSH

Cette section décrit comment configurer l'accès ASA pour HTTPS (y compris ASDM et CSM), Telnet ou SSH. Consultez les consignes suivantes :

- Pour accéder à l'interface ASA pour l'accès de gestion, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès de gestion conformément aux sections de ce chapitre. Si, toutefois, vous configurez la redirection HTTP pour rediriger automatiquement les connexions HTTP vers HTTPS, vous devez activer un critère d'accès pour autoriser HTTP; sinon, l'interface ne peut pas être à l'écoute du port HTTP.
- L'accès de gestion à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte de gestion est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe. La seule exception à cette règle est une connexion VPN. Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 14.
- L'ASA permet :
  - Un maximum de 5 connexions Telnet simultanées par contexte, si disponible, avec un maximum de 100 connexions réparties entre tous les contextes.
  - Un maximum de 5 connexions SSH simultanées par contexte, si disponible, avec un maximum de 100 connexions réparties entre tous les contextes.

- En mode de contexte unique, vous pouvez avoir un maximum de 5 sessions ASDM simultanées. En mode de contexte multiple, vous pouvez avoir un maximum de 5 sessions ASDM simultanées par contexte, avec un maximum de 200 instances ASDM parmi tous les contextes.

  Les sessions ASDM utilisent deux connexions HTTPS: une pour la surveillance qui est toujours présente et une pour apporter des modifications de configuration qui est présente uniquement lorsque vous apportez des modifications. Par exemple, la limite système en mode de contexte multiple de 200 sessions ASDM représente une limite de 400 sessions HTTPS.

- Un maximum de 6 sessions HTTPS non ASDM simultanées en mode de contexte unique ou par contexte, si disponible, avec un maximum de 100 sessions HTTPS parmi tous les contextes.

Configurer l'accès HTTPS pour ASDM, autres clients

Cette section décrit comment configurer l'accès ASA pour HTTPS, y compris ASDM et CSM.

Si vous avez activé SSL (**webvpn** > **enable** *interface*) et l'accès HTTPS sur la même interface, vous pouvez accéder à Secure Client (services client sécurisés) 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. Si vous activez également l'authentification pour HTTPS (Configurer l'authentification pour l'interface de ligne de commande ASDM et activer la commande Access, à la page 23), vous devez alors spécifier un port différent pour l'accès à ASDM.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue**Add Device Access Configuration** (Ajouter une configuration d'accès à l'appareil) apparaît.

Étape 2 Choisissez **ASDM/HTTPS**.

Étape 3 Choisissez l'interface de gestion et définissez les adresses IP d'hôte autorisées, puis cliquez sur **OK**.

Spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 14), spécifiez l'interface BVI nommée.

Étape 4 Pour exiger l'authentification par certificat, dans la zone **Specify the interface requires client certificate to access ASDM** (Spécifier l'interface exige que le certificat client accède à ASDM), cliquez sur **Add** (Ajouter) pour spécifier l'interface et une carte de certificat facultative qui doit être mise en correspondance pour une authentification réussie. Consultez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès au réseau (client))** > **Advanced (Avancé)** > **IPSec** > **Certificate to Connection Map (Certificat pour carte de connexion)** > **Rules (Règles)** pour créer la carte de certificat.

Étape 5 Configurez les **HTTP Settings** (Paramètres HTTP).

- **Enable HTTP server** (Activer le serveur HTTP) : activez le serveur HTTPS.
- **Port Number** (Numéro de port) : définissez le numéro de port. La valeur par défaut est 443.
- **Idle Timeout** (Délai d'inactivité) : définissez le délai d'inactivité pour les connexions ASDM, de 1 à 1 440 minutes. La valeur par défaut est 20 minutes. L'ASA déconnecte une connexion ASDM qui est inactive pendant la période définie.
- **Session Timeout** (Session expirée) : définissez le session expirée pour les sessions ASDM, de 1 à 1 440 minutes. Ce délai est désactivé par défaut. L'ASA déconnecte une session ASDM qui dépasse la période définie.
- **Connection Session Timeout** (Session de connexion expirée) : définissez le délai d'inactivité pour toutes les connexions HTTPS, y compris ASDM, WebVPN et d'autres clients, de 10 à 86 400 secondes. Ce délai est désactivé par défaut. L'ASA déconnecte une connexion qui est inactive pendant la période définie. Si vous définissez **Idle Timeout** (Délai d'inactivité) et **Connection Session Timeout** (Session de connexion expirée), la **Connection Session Timeout** (Session de connexion expirée) prévaut.

Étape 6 Cliquez sur **Apply** (Appliquer).

Étape 7 (Facultatif) Autorisez les clients HTTPS non basés sur le navigateur à accéder aux services HTTPS sur l'ASA. Par défaut, ASDM, CSM et l'API REST sont autorisés.

De nombreux clients spécialistes (par exemple, les bibliothèques python, curl et wget) ne prennent pas en charge l'authentification basée sur le jeton Cross-site Request Forgery (CSRF). Vous devez donc autoriser expressément ces clients à utiliser la méthode d'authentification de base ASA. Pour des raisons de sécurité, vous ne devez autoriser que les clients requis.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **HTTP Non-Browser Client Support (Prise en charge des clients HTTP non basés sur le navigateur)**, puis cliquez sur **Add** (Ajouter).

b) Dans le champ **User-Agent String from the HTTP Header** (Chaîne User-Agent de l'en-tête HTTP), spécifiez la chaîne User-Agent du client dans l'en-tête HTTP de la requête HTTP.

Vous pouvez spécifier la chaîne complète ou une chaîne partielle; les chaînes partielles doivent correspondre au début de la chaîne User-Agent. Nous conseillons d'utiliser des chaînes complètes pour une meilleure sécurité. Notez que la chaîne est sensible à la casse.

Par exemple, **`curl`** correspondra à la chaîne User-Agent suivante :

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

`curl` ne correspondra *pas* à la chaîne User-Agent suivante :

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1
Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

`CURL` ne correspondra *pas* à la chaîne User-Agent suivante :

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

Configurer l'accès SSH

Lignes directrices relatives à SSH

- Pour accéder à l'interface ASA pour l'accès SSH, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès SSH conformément à cette section.
- L'accès SSH à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte SSH est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe. La seule exception à cette règle est une connexion VPN (uniquement prise en charge par la pile ASA SSH). Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 14.
- L'ASA permet un maximum de cinq connexions SSH simultanées par contexte/mode unique, avec un maximum de 100 connexions réparties entre tous les contextes. Cependant, comme les commandes de configuration peuvent obtenir des verrouillages sur les ressources en cours de modification, vous devez apporter des modifications à une session SSH à la fois pour vous assurer que toutes les modifications sont appliquées correctement.
- Par défaut, l'ASA utilise la pile CiscoSSH, qui est basée sur OpenSSH. Vous pouvez choisir d'activer à la place la pile ASA SSH propriétaire. CiscoSSH prend en charge :
  - Conformité FIPS
  - Mises à jour régulières, y compris les mises à jour de Cisco et de la communauté de code source libre.

  Notez que la pile CiscoSSH ne prend pas en charge :
  - SSH vers une interface différente sur VPN (accès de gestion)
  - Paire de clés EDDSA
  - Paire de clés RSA en mode FIPS

  Si vous avez besoin de ces fonctionnalités, vous devez utiliser la pile SSH ASA.
- Pour utiliser la commande **copy** de l'ASA afin de copier un fichier vers ou depuis un serveur SCP, vous devez :
  - (Pile CiscoSSH uniquement) Activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP
  - Générer une paire de clés (pour les ASA physiques uniquement)
- Le nom d'utilisateur SSH par défaut n'est plus pris en charge. Vous ne pouvez plus vous connecter à l'ASA à l'aide de SSH avec le nom d'utilisateur **pix** ou **asa** et le mot de passe de connexion. Pour utiliser SSH, vous devez configurer l'authentification AAA en sélectionnant **Configuration** > **Device Management (Gestion de l'appareil)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authentication (Authentification)**; puis définissez un utilisateur local en choisissant **Configuration** > **Device Management (Gestion de l'appareil)** > **Users/AAA (Utilisateurs/AAA)**. Si vous souhaitez utiliser un serveur AAA pour l'authentification au lieu de la base de données locale, nous vous conseillons de configurer également l'authentification locale comme méthode de sauvegarde.
- Seule la version 2 du protocole SSH est prise en charge.

Pour configurer l'accès SSH à l'ASA, activez le serveur SSH et identifiez les adresses IP autorisées. Pour authentifier les utilisateurs, vous pouvez utiliser les méthodes suivantes :

- Nom d'utilisateur et mot de passe utilisant la base de données locale ou un serveur AAA.
- Nom d'utilisateur et clé publique utilisant la base de données locale.

Activer le serveur SSH

Activez le serveur SSH et spécifiez les adresses IP autorisées à se connecter. Vous pouvez également configurer d'autres paramètres du serveur SSH.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

  Pour définir la pile SSH, terminez la configuration dans l'espace système sur **Configuration** > **Device Management (Gestion des périphériques)** > **SSH Stack (Pile SSH)**.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue**Add Device Access Configuration** (Ajouter une configuration d'accès à l'appareil) apparaît.

Étape 2 Choisissez **SSH**.

Étape 3 Choisissez l'interface de gestion et définissez les adresses IP d'hôte autorisées, puis cliquez sur **OK**.

Spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 14), spécifiez l'interface BVI nommée.

Étape 4 (Facultatif) Configurez l'option **SSH Settings** (Paramètres SSH).

- **SSH Stack** (Pile SSH) : choisissez **ASA** ou **Cisco**.

Remarque En mode de contexte multiple, consultez **Configuration** > **Device Management (Gestion des périphériques)** > **SSH Stack (Pile SSH)**.

- **SSH Timeout** (Délai d'expiration SSH) : définissez le délai d'expiration entre 1 et 60 minutes. La valeur par défaut est 5 minutes. La durée par défaut est trop courte dans la plupart des cas et doit être augmentée jusqu'à ce que tous les tests et dépannages de pré-production soient terminés.
- **Key Exchange Hostkey** (Clé d'hôte pour l'échange de clés) Par défaut, l'ASA tente d'utiliser les clés dans l'ordre suivant, si elles existent :EdDSA, ECDSA, puis RSA. Si vous choisissez explicitement la clé 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 des clés RSA sera supprimée dans une version ultérieure. Nous vous suggérons donc d'utiliser les autres types de clés pris en charge.

- **DH Key Exchange** (Échange de clés DH) (Contexte d'administration uniquement) : cliquez sur le bouton radio applicable pour choisir le groupe d'échange de clés Diffie-Hellman (DH). Si aucune méthode d'échange de clés de groupe DH n'est spécifiée, la méthode d'échange de clés Groupe DH 14 SHA256 est utilisée. Pour en savoir plus sur l'utilisation des méthodes d'échange de clés DH, consultez la RFC 4253. Vous ne pouvez définir l'échange de clés que dans le contexte d'administration; cette valeur est utilisée par tous les contextes.

Étape 5 Cliquez sur **Apply** (Appliquer).

Étape 6 (Facultatif) Configurez les algorithmes de chiffrement et d'intégrité SSH :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)**.

b) Sélectionnez **Encryption** (Chiffrement), puis cliquez sur **Edit** (Modifier).

c) Dans la liste déroulante SSH cipher security level (Niveau de sécurité du chiffrement SSH), choisissez l'un des niveaux suivants.

Les chiffrements sont utilisés dans l'ordre dans lequel ils sont répertoriés. Pour les listes prédéfinies, ils sont répertoriés du plus haut au plus bas niveau de sécurité.

- **All** (Tous) : spécifie l'utilisation de tous les chiffrements : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr chacha20-poly1305@openssh.com aes192-ctr aes256-ctr
- **Custom** (Personnalisé) : spécifie une chaîne de configuration de chiffrement personnalisée que vous saisissez dans le champ **Cipher algorithms/custom string** (Algorithmes de chiffrement/Chaîne personnalisée), séparée par des deux-points.
- **Fips** : spécifie uniquement les chiffrements conformes à la norme FIPS : aes128-cbc aes256-cbc
- **High** spécifie uniquement les chiffrements de force élevée : aes256-cbc chacha20-poly1305@openssh.com aes256-ctr
- **Low** spécifie les chiffrements de force faible, moyenne et élevée : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- **Medium** : spécifie les chiffrements de force moyenne et élevée (par défaut) : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

d) Sélectionnez **Integrity** (Intégrité), puis cliquez sur **Edit** (Modifier).

e) Dans la liste déroulante SSH cipher security level (Niveau de sécurité du chiffrement SSH), choisissez l'un des niveaux suivants :

- **All** (Tous) : spécifie l'utilisation de tous les chiffrements : hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96
- **Custom** (Personnalisé) : spécifie une chaîne de configuration de chiffrement personnalisée que vous saisissez dans le champ **Cipher algorithms/custom string** (Algorithmes de chiffrement/Chaîne personnalisée), séparée par des deux-points.
- **FIPS** : spécifie uniquement les chiffrements conformes à la norme FIPS : hmac-sha1 hmac-sha2-256
- **High** (Élevé) : spécifie uniquement les chiffrements de force élevée (par défaut) : hmac-sha2-256

- **Low** (Faible) : spécifie les chiffrements de force faible, moyenne et élevée : hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96
- **Medium** (Moyen) : spécifie les chiffrements de force moyenne et élevée : hmac-sha1 hmac-sha1-96

Étape 7 Activez le serveur Secure Copy.

a) Selon votre mode de contexte :

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

b) Cochez la case **Enable secure copy server** (Activer le serveur Secure Copy).

Étape 8 Cliquez sur **Apply** (Appliquer).

Exemples

L'exemple suivant montre une session SCP vers l'ASA. À partir d'un client sur l'hôte externe, effectuez un transfert de fichiers SCP. Par exemple, dans Linux, saisissez la commande suivante :

scp -v -pw *password* [*path*/]*source_filename*
*username@asa_address***:** {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

L'option **-v** correspond à verbose (détaillé), et si **-pw** n'est pas spécifié, vous serez invité à saisir un mot de passe.

Configurer SSH pour l'accès par mot de passe

Configurez l'authentification SSH à l'aide d'un nom d'utilisateur et d'un mot de passe.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authentication (Authentification)**.

Étape 2 Cochez la case **SSH**.

Étape 3 Choisissez la base de données **LOCALE** ou un serveur AAA dans la liste déroulante **Server Group** (Groupe de serveurs).

Ce paramètre n'affecte pas l'authentification par clé publique locale pour les noms d'utilisateur qui ont une clé publique configurée. L'ASA utilise implicitement la base de données locale pour l'authentification par clé publique. Ce paramètre n'affecte que les noms d'utilisateur locaux avec mots de passe. Si vous souhaitez autoriser l'authentification par clé publique ou l'utilisation du mot de passe par un utilisateur local, vous devez configurer explicitement l'authentification locale à l'aide de ce paramètre pour autoriser l'accès par mot de passe.

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

Étape 5 Créez un utilisateur dans la base de données locale ou sur un serveur AAA qui peut être utilisé pour l'accès SSH. Consultez la procédure suivante pour ajouter un nom d'utilisateur local (conseillé).

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add User Account-Identity** (Ajouter une identité de compte d'utilisateur) apparaît.

b) Entrez un nom d'utilisateur et un mot de passe, puis confirmez le mot de passe.

Vous pouvez utiliser l'authentification par clé publique ou l'authentification par mot de passe pour le même utilisateur local. L'authentification par clé publique n'est pas prise en charge par un serveur AAA.

c) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 6 Générez une paire de clés (pour les ASA physiques uniquement).

Pour l'ASAv, les paires de clés sont automatiquement créées après le déploiement. L'ASAv ne prend en charge que la clé RSA.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**.
b) Cliquez sur **Add** (Ajouter), puis sur le bouton radio **Add a new identity certificate** (Ajouter un nouveau certificat d'identité).
c) Cliquez sur **New** (Nouveau).
d) Dans la boîte de dialogue **Add Key Pair** (Ajouter une paire de clés), précisez le type et la taille, puis cliquez sur **Generate Now** (Générer maintenant).

La paire de clés par défaut utilisée est EdDSA, ECDSAA, puis RSA. Pour RSA, choisissez une taille de 2048 bits ou plus.

Vous pouvez ensuite **annuler** dans la boîte de dialogue du certificat, car vous souhaitiez uniquement générer la paire de clés.



Remarque EdDSA n'est pas pris en charge avec la pile CiscoSSH.

e) Cliquez sur **Apply** (Appliquer).

Configurer SSH pour l'accès par clé publique

Configurez l'authentification SSH à l'aide d'une clé publique.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

Procédure

Étape 1 Créez un utilisateur dans la base de données locale qui peut être utilisé pour l'accès SSH.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add User Account-Identity** (Ajouter une identité de compte d'utilisateur) apparaît.

b) Entrez un nom d'utilisateur et un mot de passe, puis confirmez le mot de passe.

Vous pouvez créer un utilisateur sans mot de passe si vous souhaitez forcer l'utilisateur à utiliser l'authentification par clé publique au lieu de l'authentification par mot de passe. Si vous configurez l'authentification par clé publique ainsi qu'un mot de passe, l'utilisateur peut se connecter en utilisant l'une ou l'autre des méthodes si vous configurez explicitement l'authentification AAA dans cette procédure.

c) Activez l'authentification par clé publique. Choisissez l'un des volets suivants :

- **Public Key Authentication** (Authentification par clé publique) : collez une clé publique codée en Base64. Vous pouvez générer la clé à l'aide de n'importe quel logiciel de génération de clés SSH (comme ssh keygen) qui peut générer des clés brutes ssh-rsa, ssh-ed25519 ou ecdsa-sha2-nistp (sans certificats). Lorsque vous affichez une clé existante, la clé est chiffrée à l'aide d'un hachage SHA-256. Si vous devez copier et coller une clé de hachage, cochez la case **Key is hashed** (La clé est hachée).

  Pour supprimer une clé d'authentification, cliquez sur **Delete Key** (Supprimer la clé) pour afficher une boîte de dialogue de confirmation. Cliquez sur **Yes** (Oui) pour supprimer la clé d'authentification ou sur **No** (Non) pour la conserver.

- **Public Key Using PKF** (Clé publique utilisant PKF) : cochez la case **Specify a new PKF** (Spécifier une nouvelle clé PKF), et collez ou importez une clé formatée de fichier de clé publique (PKF), jusqu'à 4 096 bits. Utilisez ce format pour les clés trop importantes pour les coller au format base64. Par exemple, vous pouvez générer une clé de 4 096 bits à l'aide de ssh keygen, puis la convertir en PKF, et l'importer dans ce volet. Lorsque vous affichez une clé existante, celle-ci est chiffrée à l'aide du hachage SHA-256. Si vous devez copier et coller une clé de hachage, copiez-la à partir du volet **Public Key Authentication** (Authentification de clé publique) et collez-la dans ce volet sur le nouvel ASA avec la case **Key is hashed** (La clé de hachage) cochée.

  Pour supprimer une clé d'authentification, cliquez sur **Delete Key** (Supprimer la clé) pour afficher une boîte de dialogue de confirmation. Cliquez sur **Yes** (Oui) pour supprimer la clé d'authentification ou sur **No** (Non) pour la conserver.

d) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Étape 2 Générez une paire de clés (pour les ASA physiques uniquement).

Pour l'ASAv, les paires de clés sont automatiquement créées après le déploiement. L'ASAv ne prend en charge que la clé RSA.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**.
b) Cliquez sur **Add** (Ajouter), puis sur le bouton radio **Add a new identity certificate** (Ajouter un nouveau certificat d'identité).
c) Cliquez sur **New** (Nouveau).
d) Dans la boîte de dialogue **Add Key Pair** (Ajouter une paire de clés), précisez le type et la taille, puis cliquez sur **Generate Now** (Générer maintenant).

   La paire de clés par défaut utilisée est EdDSA, ECDSAA, puis RSA. Pour RSA, choisissez une taille de 2048 bits ou plus.

Remarque Avec la pile CiscoSSH, seule la paire de clés configurée est partagée par l'ASA au moment de l'établissement d'une connexion.

Vous pouvez ensuite **annuler** dans la boîte de dialogue du certificat, car vous souhaitiez uniquement générer la paire de clés.

Remarque EdDSA n'est pas pris en charge avec la pile CiscoSSH.

e) Cliquez sur **Apply** (Appliquer).

Exemples

L'exemple suivant montre comment s'authentifier à l'aide d'une clé au format PKF :

L'exemple suivant génère une clé partagée pour SSH sur un système Linux ou Macintosh et l'importe dans l'ASA :

1. Générez les clés publiques et privées RSA pour 4 096 bits sur votre ordinateur :

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
```

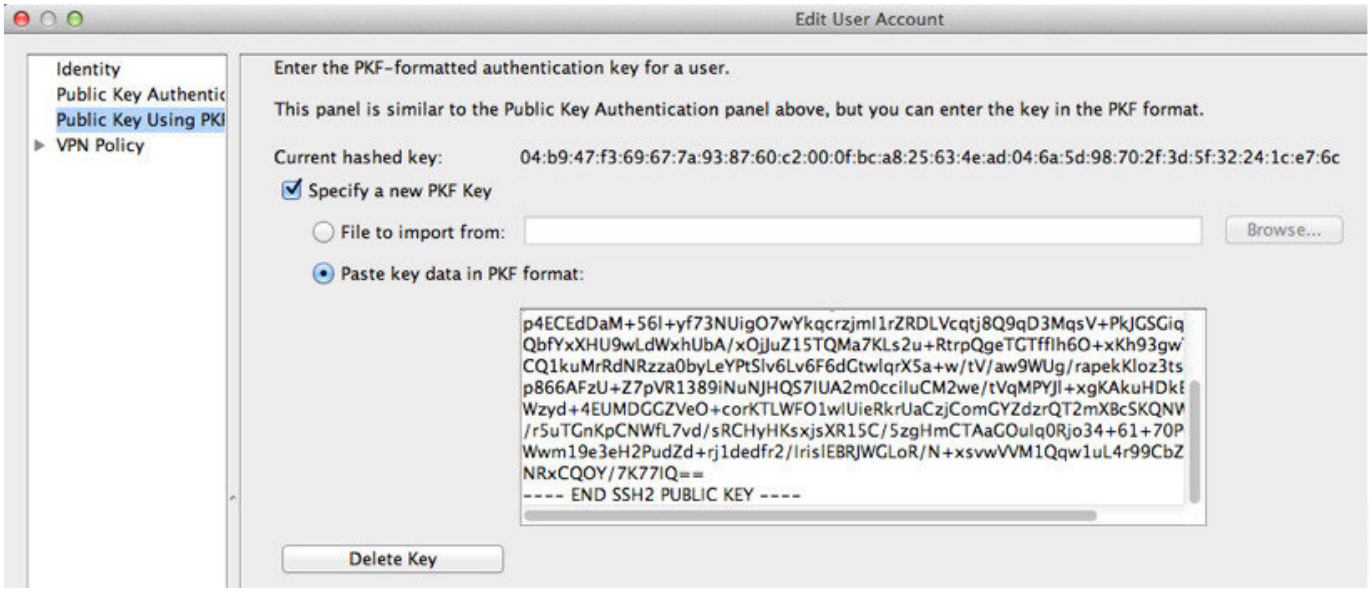
```
|   o o             |
| ooooo             |
+-------------------+
```

2. Convertissez la clé au format PKF :

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by john@jcrichton-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. Copiez la clé dans votre presse-papiers.

4. Dans ASDM, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, sélectionnez le nom d'utilisateur, puis cliquez sur **Edit** (Modifier). Cliquez sur **Public Key Using PKF** (Clé publique utilisant PKF) et collez la clé dans la fenêtre :



5. Vérifiez que l'utilisateur peut se connecter par SSH à l'ASA. Pour le mot de passe, saisissez le mot de passe de la clé SSH que vous avez spécifié lors de la création de la paire de clés.

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
```

```
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

La boîte de dialogue suivante s'affiche pour que vous puissiez saisir votre phrase secrète :



Pendant ce temps, dans la session de terminal :

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

Configurer l'accès Telnet

Cette section décrit comment configurer l'accès ASA pour Telnet. Vous ne pouvez pas utiliser Telnet sur l'interface de sécurité la plus basse, sauf si vous utilisez Telnet dans un tunnel VPN.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.
- Pour accéder à l'interface de ligne de commande d'ASA à l'aide de Telnet, saisissez le mot de passe de connexion. Vous devez définir manuellement le mot de passe avant d'utiliser Telnet.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue**Add Device Access Configuration** (Ajouter une configuration d'accès à l'appareil) apparaît.

Étape 2 Choisissez **Telnet**.

Étape 3 Choisissez l'interface de gestion et définissez les adresses IP d'hôte autorisées, puis cliquez sur **OK**.

Spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 14), spécifiez l'interface BVI nommée.

Étape 4 (Facultatif) Définissez le **Telnet Timeout** (Délai d'expiration Telnet). La valeur de délai d'expiration par défaut est de 5 minutes.

Étape 5 Cliquez sur **Apply** (Appliquer).

Étape 6 Définissez un mot de passe de connexion avant de pouvoir vous connecter à Telnet; il n'y a pas de mot de passe par défaut.

a) Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)**.
b) Cochez la case **Change the password to access the console of the security appliance** (Changer le mot de passe pour accéder à la console de l'appareil de sécurité) dans la zone **Telnet Password** (Mot de passe Telnet).
c) Entrez l'ancien mot de passe (laissez ce champ vide pour un nouvel ASA), puis entrez le nouveau mot de passe et confirmez-le.
d) Cliquez sur **Apply** (Appliquer).

Configurer la redirection HTTP pour l'accès ASDM ou le SSL VPN sans client

Vous devez utiliser HTTPS pour vous connecter à l'ASA à l'aide d'ASDM ou du SSL VPN sans client. Pour plus de commodité, vous pouvez rediriger les connexions de gestion HTTP vers HTTPS. Par exemple, en redirigeant HTTP, vous pouvez saisir **http://10.1.8.4/admin/** ou **https://10.1.8.4/admin/** et arriver toujours à la page de lancement d'ASDM à l'adresse HTTPS.

Vous pouvez rediriger le trafic IPv4 et IPv6.

Avant de commencer

Normalement, vous n'avez pas besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Cependant, pour la redirection HTTP, vous devez activer un critère d'accès pour autoriser HTTP; sinon, l'interface ne peut pas être à l'écoute du port HTTP.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **HTTP Redirect (Redirection HTTP)**.

Le tableau affiche les interfaces actuellement configurées et si la redirection est activée sur une interface.

Étape 2 Sélectionnez l'interface que vous utilisez pour ASDM et cliquez sur **Edit** (Modifier).

Étape 3 Configurez les options suivantes dans la boîte de dialogue **Edit HTTP/HTTPS Settings** (Modifier les paramètres HTTP/HTTPS) :

- **Redirect HTTP to HTTPS** (Rediriger les requêtes HTTP vers HTTPS) : redirige les requêtes HTTP vers HTTPS.

- **HTTP Port** (Port HTTP) : identifie le port à partir duquel l'interface redirige les connexions HTTP. La valeur par défaut est 80.

Étape 4 Cliquez sur **OK**.

Configurer l'accès de gestion sur un tunnel VPN

Si votre tunnel VPN se termine sur une interface, mais que vous souhaitez gérer l'ASA en accédant à une autre interface, vous devez identifier cette interface comme une interface d'accès de gestion. Par exemple, si vous saisissez l'ASA à partir de l'interface externe, cette fonctionnalité vous permet de vous connecter à l'interface interne à l'aide d'ASDM, SSH, ou Telnet; ou vous pouvez envoyer un message Ping à l'interface interne en entrant à partir de l'interface externe.

Remarque Cette fonctionnalité n'est pas prise en charge pour SSH si vous utilisez la pile CiscoSSH, qui est la valeur par défaut.

Remarque Cette fonctionnalité n'est pas prise en charge pour SNMP. Pour SNMP sur VPN, nous vous recommandons d'activer SNMP sur une interface de boucle avec retour. Vous n'avez pas besoin d'activer la fonctionnalité d'accès de gestion pour utiliser SNMP sur l'interface de boucle avec retour. La boucle avec retour fonctionne également pour SSH.

L'accès VPN à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre accès VPN se trouve sur l'interface externe, vous pouvez uniquement initier une connexion directement à l'interface externe. Vous devez activer le VPN sur l'interface directement accessible de l'ASA et utiliser la résolution de noms pour ne pas avoir à vous souvenir de plusieurs adresses.

L'accès de gestion est disponible par les types de tunnel VPN suivants : clients IPsec, IPsec de site à site, Easy VPN et le SSL VPN Secure Client (services client sécurisés).

Avant de commencer

- Cette fonctionnalité n'est pas prise en charge sur les interfaces de gestion uniquement.
- Lorsque vous utilisez une interface d'accès de gestion et que vous configurez la NAT d'identité, vous devez configurer la NAT avec l'option de recherche de routage. Pour en savoir plus, consultez la section « Accès à la gestion de la NAT et du VPN » dans le chapitre *Exemples de NAT et référence* dans la version appropriée du Guide de configuration de l'interface de ligne de commande du pare-feu ASA.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Management Interface (Interface de gestion)**.

Étape 2 Choisissez l'interface ayant la sécurité la plus élevée (l'interface interne) dans la liste déroulante **Management Access Interface** (Interface d'accès de gestion).

Pour Site à site, vous pouvez spécifier une BVI nommée (en mode routé).

Étape 3 Cliquez sur **Apply** (Appliquer).

L'interface de gestion est attribuée et la modification est enregistrée dans la configuration d'exécution.

Configurer l'accès de gestion pour FXOS sur les interfaces de données en mode plateforme Firepower 2100

Si vous souhaitez gérer FXOS sur le Firepower 2100 en mode plateforme à partir d'une interface de données, vous pouvez configurer l'accès SSH, HTTPS et SNMP. Cette fonctionnalité est utile si vous souhaitez gérer le périphérique à distance, mais que vous souhaitez conserver la gestion 1/1, qui est la méthode d'accès native à FXOS, sur un réseau isolé. Si vous activez cette fonctionnalité, vous pouvez continuer à utiliser l'interface de gestion Management 1/1 pour l'accès local uniquement. Cependant, vous ne pouvez pas autoriser l'accès *à distance* depuis ou vers l'interface de gestion Management 1/1 pour FXOS en même temps que l'utilisation de cette fonctionnalité. Cette fonctionnalité nécessite le transfert du trafic vers les interfaces de données ASA à l'aide d'un chemin interne (valeur par défaut), et vous ne pouvez spécifier qu'une seule passerelle de gestion FXOS.

L'ASA utilise des ports non standard pour l'accès FXOS; le port standard est réservé à l'utilisation par l'ASA sur la même interface. Lorsque l'ASA transfère le trafic vers FXOS, il traduit le port de destination non standard en port FXOS pour chaque protocole (ne modifiez pas le port HTTPS dans FXOS). L'adresse IP de destination du paquet (qui est l'adresse IP de l'interface ASA) est également convertie en une adresse interne pour l'utilisation par FXOS. L'adresse source reste inchangée. Pour renvoyer le trafic, l'ASA utilise sa table de routage de données pour déterminer la bonne interface de sortie. Lorsque vous accédez à l'adresse IP de données ASA pour l'application de gestion, vous devez vous connecter en utilisant un nom d'utilisateur FXOS; les noms d'utilisateur ASA ne s'appliquent qu'à l'accès de gestion ASA.

Vous pouvez également activer l'*initiation* du trafic de gestion FXOS sur les interfaces de données ASA. Cette fonction est requise pour les alertes SNMP ou pour l'accès au serveur NTP et DNS, par exemple. Par défaut, l'initiation du trafic de gestion FXOS est activée pour l'interface externe ASA pour la communication avec les serveurs DNS et NTP (cette fonctionnalité est requise pour la communication avec les licences Smart).

Avant de commencer

- Mode contexte unique seulement.
- Exclut les interfaces de gestion ASA uniquement.
- Vous ne pouvez pas utiliser un tunnel VPN pour l'interface de données ASA et accéder directement à FXOS. Comme solution de contournement pour SSH, vous pouvez faire appel au VPN vers l'ASA, accéder à l'interface de ligne de commande de l'*ASA*, puis utiliser la commande **connect fxos** pour accéder à l'interface de ligne de commande de FXOS. Notez que SSH, HTTPS et SNMPv3 sont/peuvent être chiffrés, de sorte qu'une connexion directe à l'interface de données est sécurisée.
- Assurez-vous que la passerelle FXOS est configurée pour acheminer le trafic vers les interfaces de données ASA (par défaut). Consultez le guide de démarrage pour en savoir plus sur la configuration de la passerelle.

Procédure

Étape 1 Dans ASDM, choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **FXOS Remote Management (Gestion à distance FXOS)**.

Étape 2 Activez la gestion à distance FXOS.

a) Choisissez **HTTPS**, **SNMP** ou **SSH** dans le volet de navigation.

b) Cliquez sur **Add** (ajouter) et définissez l'**interface** sur laquelle vous souhaitez autoriser la gestion, définissez l'adresse IP (**IP Address**) autorisée pour la connexion, puis cliquez sur **OK**.

Vous pouvez créer plusieurs entrées pour chaque type de protocole. Définissez le **port** si vous ne souhaitez pas utiliser les paramètres par défaut suivants :

- Port HTTPS par défaut : 3443
- Port SNMP par défaut : 3061
- Port SSH par défaut : 3022

Étape 3 Permettez à FXOS d'initier des connexions de gestion à partir de l'interface ASA.

a) Choisissez **FXOS Traffic Initiation** (initialisation du trafic FXOS) dans le volet de navigation.

b) Cliquez sur **Add** et activez les interfaces ASA par lesquelles vous devez envoyer le trafic de gestion FXOS. Par défaut, l'interface externe est activée.

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

Étape 5 Connectez-vous à Firewall Chassis Manager sur l'interface de gestion Management 1/1 (par défaut https://192.168.45.45, avec le nom d'utilisateur : **admin** et le mot de passe : **Admin123**).

Étape 6 Cliquez sur l'onglet **Platform Settings** (paramètres de plateforme) et activez **SSH**, **HTTPS** ou **SNMP**.

SSH et HTTPS sont activés par défaut.

Étape 7 Configurez une liste d'accès (**Access List**) dans l'onglet des paramètres de la plateforme (**Platform Settings**) pour autoriser vos adresses de gestion. SSH et HTTPS autorisent uniquement le réseau de gestion Management 1/1 192.168.45.0 par défaut. Vous devez autoriser toutes les adresses que vous avez spécifiées dans la configuration de gestion à distance FXOS (**FXOS Remote Management**) sur l'ASA.

Modifier le délai d'expiration de la console

Le délai d'expiration de la console définit combien de temps une connexion peut rester en mode d'exécution privilégié ou en mode de configuration; une fois le délai d'expiration atteint, la session passe en mode EXEC de l'utilisateur. Par défaut, la session n'expire pas. Ce paramètre n'a pas d'incidence sur la durée de votre connexion au port de console, qui n'expire jamais.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Command Line (CLI) (Ligne de commande (interface de ligne de commande))** > **Console Timeout (Délai d'expiration de la console)**.

Étape 2 Définissez une nouvelle valeur de délai d'expiration en minutes. Pour spécifier une durée illimitée, saisissez **0**. La valeur par défaut est 0.

Étape 3 Cliquez sur **Apply** (Appliquer).

La modification de la valeur du délai d'expiration est enregistrée dans la configuration en cours d'exécution.

Personnaliser une invite de l'interface de ligne de commande

La possibilité d'ajouter des renseignements à une invite vous permet de voir en un coup d'œil à quel ASA vous êtes connecté lorsque vous avez plusieurs modules. Lors d'un basculement, cette fonctionnalité est utile lorsque les deux ASA ont le même nom d'hôte.

En mode de contexte multiple, vous pouvez afficher l'invite étendue lorsque vous vous connectez à l'espace d'exécution du système ou au contexte d'administration. Dans un contexte de non-administration, vous ne voyez que l'invite par défaut, qui est le nom d'hôte et le nom de contexte.

Par défaut, l'invite affiche le nom d'hôte de l'ASA. En mode de contexte multiple, l'invite affiche également le nom du contexte. Vous pouvez afficher les éléments suivants dans l'invite de l'interface de ligne de commande :

cluster-unit	Affiche le nom de l'unité de grappe. Chaque unité d'une grappe peut avoir un nom unique.
context	(Mode multiple uniquement) Affiche le nom du contexte actuel.
domaine	Affiche le nom de domaine.
hostname	Affiche le nom d'hôte.
priority	Affiche la priorité de basculement comme pri (principal) ou sec (secondaire).

state	Affiche l'état de transmission du trafic ou le rôle de l'unité. Pour le basculement, les valeurs suivantes sont affichées pour le mot clé d'état : • **act** : le basculement est activé et l'unité transmet activement le trafic. • **stby** : le basculement est activé et l'unité ne transmet pas de trafic et est en veille, en panne ou dans un autre état non actif. • **actNoFailover** : le basculement n'est pas activé et l'unité transmet activement le trafic. • **stbyNoFailover** : le basculement n'est pas activé et l'unité ne transmet pas de trafic. Cela pourrait se produire en cas de défaillance d'interface au-dessus du seuil sur l'unité en veille. Pour la mise en grappe, les valeurs du contrôle et des données sont affichées.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Command Line (CLI) (Ligne de commande (interface de ligne de commande))** > **CLI Prompt (Invite de l'interface de ligne de commande).**

Étape 2 Effectuez l'une des opérations suivantes pour personnaliser l'invite :

- Cliquez sur l'attribut dans la liste **Available Prompts** (Invites disponibles), puis cliquez sur **Add** (Ajouter). Vous pouvez ajouter plusieurs attributs à l'invite. L'attribut est déplacé de la liste **Available Prompts** (Invites disponibles) vers la liste **Selected Prompts** (Invites sélectionnées).
- Cliquez sur l'attribut dans la liste **Selected Prompts** (Invites sélectionnées), puis cliquez sur **Delete** (Supprimer). L'attribut est déplacé de la liste **Selected Prompts** (Invites sélectionnées) vers la liste **Available Prompts** (Invites disponibles).
- Cliquez sur l'attribut dans la liste **Selected Prompts** (Invites sélectionnées), puis sur **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas) pour modifier l'ordre dans lequel les attributs s'affichent.

L'invite est modifiée et s'affiche dans le champ **CLI Prompt Preview** (Aperçu de l'invite de l'interface de ligne de commande).

Étape 3 Cliquez sur **Apply**.

La nouvelle invite est enregistrée dans la configuration d'exécution.

Configurer une bannière de connexion

Vous pouvez configurer un message pour qu'il s'affiche lorsqu'un utilisateur se connecte à l'ASA, avant qu'un utilisateur ne se connecte ou avant qu'un utilisateur n'entre en mode d'exécution privilégié.

- Du point de vue de la sécurité, il est important que votre bannière dissuade les accès non autorisés. N'utilisez pas les mots « bienvenue » ou « s'il vous plaît », car ils semblent inviter des intrus à entrer. La bannière suivante donne le bon ton en cas d'accès non autorisé :

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- Après l'ajout d'une bannière, les sessions Telnet ou SSH à l'ASA peuvent se fermer si :
  - La mémoire système est insuffisante pour traiter les messages sur bannière.
  - Une erreur d'écriture TCP se produit lors de la tentative d'affichage des messages sur bannière.
- Consultez la RFC 2196 pour connaître les lignes directrices relatives aux messages sur bannière.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Command Line (CLI) (Ligne de commande (interface de ligne de commande))** > **Banner (Bannière)**.

Étape 2 Ajoutez le texte de votre bannière dans le champ du type de bannière que vous créez pour l'interface de ligne de commande :

- La bannière de session (exec) apparaît lorsqu'un utilisateur accède au mode d'exécution privilégié au niveau de l'interface de ligne de commande.
- La bannière de connexion apparaît lorsqu'un utilisateur se connecte à l'interface de ligne de commande.
- La bannière du message du jour (motd) s'affiche lorsqu'un utilisateur se connecte à l'interface de ligne de commande pour la première fois.
- La bannière ASDM apparaît lorsqu'un utilisateur se connecte à ASDM, après son authentification. L'utilisateur dispose de deux options pour ignorer la bannière :
  - **Continue** (Continuer) : ignorer la bannière et terminer la connexion.
  - **Disconnect** (Se déconnecter) : ignorer la bannière et terminer la connexion.
- Seuls les caractères ASCII sont autorisés, y compris une nouvelle ligne (Entrée), qui compte comme deux caractères.
- N'utilisez pas les onglets dans la bannière, car ils ne sont pas conservés dans la version de l'interface de ligne de commande.
- Il n'y a aucune limite de longueur pour les bannières autres que celles de la RAM et de la mémoire flash.
- Vous pouvez ajouter de manière dynamique le nom d'hôte ou le nom de domaine de l'ASA en incluant les chaînes **$(hostname)** et **$(domain)**.
- Si vous configurez une bannière dans la configuration système, vous pouvez utiliser ce texte de bannière dans un contexte en utilisant la chaîne **$(system)** dans la configuration du contexte.

Étape 3 Cliquez sur **Apply** (Appliquer).

La nouvelle bannière est enregistrée dans la configuration d'exécution.

Définir un quota de sessions de gestion

Vous pouvez établir un nombre maximum de sessions ASDM, SSH et Telnet simultanées qui sont autorisées sur l'ASA. Si le maximum est atteint, aucune session supplémentaire n'est autorisée et un message de journal système est généré. Pour empêcher un verrouillage du système, le mécanisme de quota de sessions de gestion ne peut pas bloquer une session de console.



Remarque En mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions ASDM, où le maximum est fixe à 5 sessions.



Remarque Si vous définissez également une limite de ressources par contexte pour le nombre maximum de sessions administratives (SSH, etc.), la valeur la plus basse sera utilisée.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet **Configuration** > **Device List (Liste des périphériques)**, cliquez deux fois sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Management Session Quota (Quota de sessions de gestion)**

Étape 2 Saisissez le nombre maximum de sessions simultanées.

- **Aggregate** (Agrégé) : définit le nombre agrégé de sessions entre 1 et 15. La valeur par défaut est de 15.
- **HTTP Sessions** (Sessions HTTP) : définit le nombre maximum de sessions HTTPS (ASDM), entre 1 et 5. La valeur par défaut est égale à 5.
- **SSH Sessions** (Sessions SSH) : définit le nombre maximum de sessions SSH, entre 1 et 5. La valeur par défaut est égale à 5.
- **Telnet Sessions** (Sessions Telnet) : définit le nombre maximum de sessions Telnet, entre 1 et 5. La valeur par défaut est égale à 5.
- **User Sessions** (Sessions d'utilisateur) : définit le nombre maximum de sessions par utilisateur, entre 1 et 5. La valeur par défaut est égale à 5.

Étape 3 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications de configuration.

Configurer AAA pour les administrateurs système

Cette section décrit comment configurer l'authentification, l'autorisation de gestion et l'autorisation de commande pour les administrateurs système.

Configurer l'authentification de gestion

Configurez l'authentification pour l'accès à l'interface de ligne de commande et à ASDM.

À propos de l'authentification de gestion

La façon dont vous vous connectez à l'ASA dépend de si vous activez ou non l'authentification.

À propos de l'authentification SSH

Consultez le comportement suivant pour l'accès SSH avec et sans authentification :

- Aucune authentification : SSH n'est pas disponible sans authentification.
- Authentification : lorsque vous activez l'authentification SSH, vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données locale des utilisateurs. Pour l'authentification par clé publique, l'ASA ne prend en charge que la base de données locale. Si vous configurez l'authentification par clé publique SSH, l'ASA utilise implicitement la base de données locale. Il vous suffit de configurer explicitement l'authentification SSH lorsque vous utilisez un nom d'utilisateur et un mot de passe pour vous connecter. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'authentification Telnet

Consultez le comportement suivant pour l'accès Telnet avec et sans authentification :

- Aucune authentification : si vous n'activez aucune authentification pour Telnet, vous ne saisissez pas de nom d'utilisateur; vous saisissez le mot de passe de connexion. Il n'y a pas de mot de passe par défaut, vous devez donc en définir un avant de pouvoir vous connecter à l'ASA via Telnet. Vous accédez au mode EXEC de l'utilisateur.
- Authentification : si vous activez l'authentification Telnet, vous saisissez le nom d'utilisateur et le mot de passe définis sur le serveur AAA ou la base de données des utilisateurs locale. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'authentification ASDM

Consultez le comportement suivant pour l'accès ASDM avec et sans authentification. Vous pouvez également configurer l'authentification par certificat, avec ou sans authentification AAA.

- Aucune authentification : par défaut, vous pouvez vous connecter à ASDM avec un nom d'utilisateur vide et le mot de passe d'activation, qui est vide par défaut. Nous vous suggérons de modifier le mot de passe d'activation dès que possible afin qu'il ne reste pas vide; voir Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet. Lorsque vous saisissez la commande **enable** au niveau de l'interface de ligne de commande pour la première fois, vous êtes invité à modifier

le mot de passe; ce comportement n'est pas appliqué lorsque vous vous connectez à ASDM. Notez que si vous saisissez un nom d'utilisateur et un mot de passe à l'écran de connexion (au lieu de laisser le nom d'utilisateur vide), ASDM vérifie la base de données locale à la recherche d'une correspondance.

- Authentification par certificat : (mode unique et routé uniquement) Vous pouvez exiger que l'utilisateur ait un certificat valide. Saisissez le nom d'utilisateur et le mot de passe du certificat pour que l'ASA valide le certificat par rapport au point de confiance PKI.
- Authentification AAA : lorsque vous activez l'authentification ASDM (HTTPS), vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données locale des utilisateurs. Vous ne pouvez plus utiliser ASDM avec un nom d'utilisateur vide et le mot de passe d'activation.
- Authentification AAA plus authentification par certificat : (mode unique et routé uniquement) Lorsque vous activez l'authentification ASDM (HTTPS), vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Si le nom d'utilisateur et le mot de passe sont différents pour l'authentification par certificat, vous êtes invité à les saisir également. Vous pouvez choisir de préremplir le nom d'utilisateur dérivé de votre certificat.

À propos de l'authentification série

Consultez le comportement suivant pour l'accès au port de console série avec et sans authentification :

- Aucune authentification : si vous n'activez aucune authentification pour l'accès en série, vous ne saisissez pas de nom d'utilisateur ni de mot de passe. Vous accédez au mode EXEC de l'utilisateur.
- Authentification : si vous activez l'authentification pour l'accès en série, vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'activation de l'authentification

Pour passer en mode d'exécution privilégié après la connexion, saisissez la commande **enable**. Le fonctionnement de cette commande dépend de si vous activez ou non l'authentification.

- Aucune authentification : si vous ne configurez pas l'authentification, saisissez le mot de passe d'activation du système lorsque vous saisissez la commande **enable**, qui est vide par défaut. La première fois que vous saisissez la commande **enable**, vous devez modifier le mot de passe. Cependant, si vous n'utilisez pas l'activation de l'authentification, après avoir saisi la commande **enable**, vous n'êtes plus connecté en tant qu'utilisateur particulier, ce qui peut affecter les fonctionnalités basées sur l'utilisateur telles que l'autorisation de commande. Pour conserver votre nom d'utilisateur, utilisez l'activation de l'authentification.
- Authentification : si vous configurez l'activation de l'authentification, l'ASA vous invite à entrer votre nom d'utilisateur et mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Cette fonctionnalité est particulièrement utile lorsque vous effectuez une autorisation de commande, dans laquelle les noms d'utilisateur sont importants pour déterminer les commandes qu'un utilisateur peut saisir.

Pour activer l'authentification à l'aide de la base de données locale, vous pouvez utiliser la commande **login** au lieu de la commande **enable**. La commande **login** conserve le nom d'utilisateur, mais ne nécessite aucune configuration pour activer l'authentification.

Mise en garde Si vous ajoutez à la base de données locale des utilisateurs qui peuvent accéder à l'interface de ligne de commande et que vous ne souhaitez pas entrer en mode d'exécution privilégié, vous devez configurer l'autorisation de commande. Sans autorisation de commande, les utilisateurs peuvent accéder au mode d'exécution privilégié (et à toutes les commandes) au niveau de l'interface de ligne de commande en utilisant leur propre mot de passe si leur niveau de privilège est de 2 ou plus (2 est la valeur par défaut). Vous pouvez également décourager l'utilisation de la commande login en utilisant un serveur AAA pour l'authentification au lieu de la base de données locale, ou vous pouvez définir tous les utilisateurs locaux au niveau 1 afin de pouvoir contrôler qui peut utiliser le mot de passe d'activation du système pour accéder au mode d'exécution privilégié.

Sessions du système d'exploitation hôte vers l'ASA

Certaines plateformes prennent en charge l'exécution de l'ASA en tant qu'application distincte : par exemple l'ASA sur le Firepower 4100/9300. Pour les sessions du système d'exploitation hôte à l'ASA, vous pouvez configurer l'authentification série et Telnet, selon le type de connexion. Par exemple, la commande **connect asa** dans FXOS sur le Firepower 2100 en mode plateforme utilise un port série.

En mode de contexte multiple, vous ne pouvez pas configurer de commandes AAA dans la configuration système. Cependant, si vous configurez l'authentification Telnet ou série dans le contexte d'administration, l'authentification s'applique également à ces sessions. Le serveur AAA du contexte d'administration ou la base de données locale des utilisateurs est utilisé dans cette instance.

Configurer l'authentification pour l'interface de ligne de commande ASDM et activer la commande Access

Avant de commencer

- Configurez l'accès Telnet, SSH ou HTTP.
- Pour l'authentification extérieure, configurez un groupe de serveurs AAA. Pour l'authentification locale, ajoutez des utilisateurs à la base de données locale.
- L'authentification de gestion HTTP ne prend pas en charge le protocole SDI pour un groupe de serveurs AAA.
- Cette fonctionnalité n'affecte pas l'authentification par clé publique SSH pour les noms d'utilisateur locaux avec la commande **ssh authentication**. L'ASA utilise implicitement la base de données locale pour l'authentification par clé publique. Cette fonctionnalité n'affecte que les noms d'utilisateur avec mots de passe. Si vous souhaitez autoriser l'authentification par clé publique ou l'utilisation du mot de passe par un utilisateur local, vous devez configurer explicitement l'authentification locale à l'aide de cette procédure pour autoriser l'accès par mot de passe.

Procédure

Étape 1 Pour authentifier les utilisateurs qui utilisent la commande **enable**, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authentication (Authentification)**, puis configurez les paramètres suivants :

a) Cochez la case **Enable** (activer).
b) Choisissez un nom de groupe de serveurs ou la base de données LOCAL.
c) (Facultatif) Si vous avez choisi un serveur AAA, vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Cochez la case **Use LOCAL when server group fails** (Utiliser LOCAL en cas d'échec du groupe de serveurs). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée.

Étape 2 Pour authentifier les utilisateurs qui accèdent à l'interface de ligne de commande ou à ASDM, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authentication (Authentification)**, puis configurez les paramètres suivants :

a) Cochez une ou plusieurs des cases suivantes :

- **HTTP/ASDM** : authentifie le client ASDM qui accède à l'ASA à l'aide de HTTPS.
- **Serial** (Série) : authentifie les utilisateurs qui accèdent à l'ASA à l'aide du port de console. Pour Firepower 2100 en mode plateforme, ce mot clé affecte la console virtuelle accessible à partir de FXOS à l'aide de la commande **connect asa**.
- **SSH** : authentifie les utilisateurs qui accèdent à l'ASA à l'aide de SSH (mot de passe uniquement; l'authentification par clé publique utilise implicitement la base de données locale).
- **Telnet** : authentifie les utilisateurs qui accèdent à l'ASA à l'aide de Telnet.

b) Pour chaque service que vous avez vérifié, choisissez un nom de groupe de serveurs ou la base de données LOCAL.
c) (Facultatif) Si vous avez choisi un serveur AAA, vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Cochez la case **Use LOCAL when server group fails** (Utiliser LOCAL en cas d'échec du groupe de serveurs). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée.

Étape 3 Cliquez sur **Apply** (Appliquer).

Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion

L'ASA vous permet de distinguer les utilisateurs administratifs et d'accès à distance lorsqu'ils s'authentifient. La différence des rôles d'utilisateur peut empêcher les utilisateurs du VPN d'accès à distance et de l'accès réseau d'établir une connexion administrative à l'ASA.

Avant de commencer

Utilisateurs RADIUS ou LDAP (mappés)

Lorsque les utilisateurs sont authentifiés par LDAP, les attributs LDAP natifs et leurs valeurs peuvent être mappés aux attributs ASA pour fournir des fonctionnalités d'autorisation spécifiques. Configurez Cisco VSA CVPN3000-Privilege-Level avec une valeur comprise entre 0 et 15, puis mappez les attributs LDAP à Cisco VAS CVPN3000-Privilege-Level.

L'attribut **service-type** IETF RADIUS, lorsqu'il est envoyé dans un message d'acceptation de l'accès à la suite d'une demande d'authentification et d'autorisation RADIUS, est utilisé pour désigner le type de service accordé à l'utilisateur authentifié.

L'attribut **privilege-level** RADIUS Cisco VSA (ID de fournisseur 3076, sous-ID 220), lorsqu'il est envoyé dans un message d'acceptation de l'accès, est utilisé pour désigner le niveau de privilège de l'utilisateur.

Utilisateurs TACACS+

L'autorisation est demandée par « service=shell », et le serveur répond par PASS (réussite) ou FAIL (échec).

Utilisateurs locaux

Configurez l'option **Access Restriction** (Restriction d'accès) pour un nom d'utilisateur donné. Par défaut, la restriction d'accès est **Full Access** (Accès complet), ce qui permet un accès complet à tous les services spécifiés par les options de l'onglet **Authentication** (Authentification).

Attributs d'autorisation de gestion

Consultez le tableau suivant pour connaître les types de serveurs AAA et les valeurs valides pour l'autorisation de gestion. L'ASA utilise ces valeurs pour déterminer le niveau d'accès de gestion.

Niveau de gestion	Attributs RADIUS/LDAP (mappés)	Attributs TACACS+	Attributs de la base de données locale
Accès complet : permet un accès complet à tous les services spécifiés par les commandes options de l'onglet **Authentication** (Authentification).	Type de service 6 (Administrateur), niveau de privilège 1	PASS (réussite), privilège de niveau 1	admin
Accès partiel : permet l'accès à l'interface de ligne de commande ou à ASDM lorsque vous configurez les commandes options de l'onglet **Authentication** (Authentification). Cependant, si vous configurez l'authentification **enable** avec la commande **Enable**, l'utilisateur de l'interface de ligne de commande ne peut pas accéder au mode d'exécution privilégié à l'aide de la commande **enable**.	Type de service 7 (invite NAS), niveau de privilège 2 et supérieur Les types de service Framed (2) et Login (1) sont traités de la même manière.	PASS (réussite), niveau de privilège 2 et supérieur	nas-prompt
Aucun accès : refuse l'accès de gestion. L'utilisateur ne peut pas utiliser les services spécifiés par les commandes options de l'onglet **Authentication** (Authentification) (à l'exception du mot clé **Serial** (Série); l'accès en série est autorisé). Les utilisateurs d'accès à distance (IPsec et SSL) peuvent toujours s'authentifier et mettre fin à leurs sessions d'accès à distance. Tous les autres types de services (voix, FAX, etc.) sont traités de la même manière.	Type de service 5 (sortant)	ÉCHEC	remote-access

Directives supplémentaires

- L'accès à la console de série n'est pas inclus dans l'autorisation de gestion.

- Vous devez également configurer l'authentification AAA pour l'accès de gestion afin d'utiliser cette fonctionnalité. Consultez Configurer l'authentification pour l'interface de ligne de commande ASDM et activer la commande Access, à la page 23.
- Si vous utilisez l'authentification extérieure, vous devez préconfigurer un groupe de serveurs AAA avant d'activer cette fonctionnalité.
- L'autorisation HTTP est prise en charge uniquement en mode routé simple.

Procédure

Étape 1 Pour activer l'autorisation de gestion des sessions HTTP, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)** et cochez la case **HTTP** dans la zone **Enable Authorization for ASA Command Access** (Activer l'autorisation pour l'accès à la commande ASA).

Remarque Pour configurer l'accès à la commande ASA, consultez Configurer l'autorisation de commande locale, à la page 28.

Étape 2 Pour activer l'autorisation de gestion des sessions Telnet et SSH, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)** et cochez la case **Enable** (Activer) dans la zone **Perform authorization for exec shell access** (Effectuer l'autorisation pour l'accès au shell d'exécution).

Étape 3 Sélectionnez les boutons radio **Remote** (Distant) ou **Local** afin de spécifier le serveur à utiliser pour l'autorisation de l'accès au shell d'exécution.

Étape 4 Pour activer l'autorisation de gestion, cochez la case **Allow privileged users to enter into EXEC mode on login** (Autoriser les utilisateurs privilégiés à entrer en mode EXEC lors de la connexion).

L'option **auto-enable** permet aux utilisateurs disposant d'un accès complet d'être placés directement en mode d'exécution privilégié. Sinon, les utilisateurs sont placés en mode EXEC utilisateur.

Configurer l'autorisation de commande

Si vous souhaitez contrôler l'accès aux commandes, l'ASA vous permet de configurer l'autorisation de commande, dans laquelle vous pouvez déterminer quelles commandes sont disponibles pour un utilisateur. Par défaut, lorsque vous vous connectez, vous pouvez accéder au mode EXEC de l'utilisateur, qui n'offre que des commandes minimales. Lorsque vous saisissez la commande **enable** (ou la commande **login** lorsque vous utilisez la base de données locale), vous pouvez accéder au mode d'exécution privilégié et aux commandes avancées, y compris les commandes de configuration.

Vous pouvez utiliser l'une des deux méthodes d'autorisation de commande suivantes :

- Niveaux de privilèges locaux
- Niveaux de privilèges du serveur TACACS+

À propos de l'autorisation de commande

Vous pouvez activer l'autorisation de commande pour que seuls les utilisateurs autorisés puissent saisir des commandes.

Méthodes d'autorisation de commande prises en charge

Vous pouvez utiliser l'une des deux méthodes d'autorisation de commande suivantes :

- Niveaux de privilèges locaux : configurez les niveaux de privilège de commande sur l'ASA. Lorsqu'un utilisateur local, RADIUS ou LDAP (si vous mappez des attributs LDAP aux attributs RADIUS) s'authentifie pour l'accès à l'interface de ligne de commande, l'ASA place cet utilisateur au niveau de privilège défini par la base de données locale, RADIUS ou le serveur LDAP. L'utilisateur peut accéder aux commandes au niveau de privilège attribué et en dessous. Notez que tous les utilisateurs accèdent au mode EXEC lorsqu'ils se connectent pour la première fois (commandes au niveau 0 ou 1). L'utilisateur doit s'authentifier de nouveau avec la commande **enable** pour accéder au mode d'exécution privilégié (commandes de niveau 2 ou supérieur), ou il peut se connecter avec la commande **login** (base de données locale uniquement).

Remarque Vous pouvez utiliser l'autorisation de commande locale sans aucun utilisateur dans la base de données locale et sans interface de ligne de commande ni authentification **enable**. Au lieu de cela, lorsque vous saisissez la commande **enable**, vous saisissez le mot de passe d'activation du système et l'ASA vous place au niveau 15. Vous pouvez ensuite créer des mots de passe d'activation pour chaque niveau, de sorte que lorsque vous entrez **enable** *n* (2 à 15), l'ASA vous place au niveau *n*. Ces niveaux ne sont pas utilisés, sauf si vous activez l'autorisation de commande locale.

- Niveaux de privilège du serveur TACACS+ : sur le serveur TACACS+, configurez les commandes qu'un utilisateur ou un groupe peut utiliser après s'être authentifié pour l'accès à l'interface de ligne de commande. Chaque commande qu'un utilisateur saisit au niveau de l'interface de ligne de commande est validée auprès du serveur TACACS+.

Contextes de sécurité et autorisation de commande

Les paramètres AAA sont distincts par contexte et ne sont pas partagés entre les contextes.

Lors de la configuration de l'autorisation de commande, vous devez configurer chaque contexte de sécurité séparément. Cette configuration vous offre la possibilité d'appliquer différentes autorisations de commande pour différents contextes de sécurité.

Lorsqu'ils passent d'un contexte de sécurité à l'autre, les administrateurs doivent savoir que les commandes autorisées pour le nom d'utilisateur spécifié lors de la connexion peuvent être différentes dans la nouvelle session de contexte ou que l'autorisation de commande peut ne pas être configurée du tout dans le nouveau contexte. Ne pas comprendre que les autorisations de commande peuvent différer d'un contexte de sécurité à l'autre peut dérouter un administrateur.

Remarque L'espace d'exécution du système ne prend pas en charge les commandes AAA; par conséquent, l'autorisation de commande n'est pas disponible dans l'espace d'exécution du système.

Niveaux de privilège de commande

Par défaut, les commandes suivantes sont affectées au niveau de privilège 0. Toutes les autres commandes sont affectées au niveau de privilège 15.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

Si vous déplacez des commandes de mode de configuration à un niveau inférieur à 15, veillez également à déplacer la commande **configure** à ce niveau, sinon l'utilisateur ne pourra pas entrer en mode de configuration.

Configurer l'autorisation de commande locale

L'autorisation de commande locale vous permet d'affecter des commandes à l'un des 16 niveaux de privilège (0 à 15). Par défaut, chaque commande est affectée au niveau de privilège 0 ou 15. Vous pouvez définir chaque utilisateur comme étant à un niveau de privilège spécifique, et chaque utilisateur peut saisir n'importe quelle commande au niveau de privilège attribué ou en dessous. L'ASA prend en charge les niveaux de privilège d'utilisateur définis dans la base de données locale, un serveur RADIUS ou un serveur LDAP (si vous mappez des attributs LDAP aux attributs RADIUS).

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)**.

Étape 2 Cochez la case **Enable authorization for ASA command access (Activer l'autorisation pour l'accès à la commande ASA)** > **Enable (Activer)**.

Étape 3 Choisissez **LOCAL** dans la liste déroulante **Server Group** (Groupe de serveurs).

Étape 4 Lorsque vous activez l'autorisation de commande locale, vous avez la possibilité d'attribuer manuellement les niveaux de privilège aux commandes individuelles ou à des groupes de commandes, ou d'activer les privilèges de compte d'utilisateur prédéfinis.

- Cliquez sur **Set ASDM Defined User Roles** (Définir les rôles d'utilisateur définis par ASDM) pour utiliser les privilèges de compte d'utilisateur prédéfinis.

La boîte de dialogue **ASDM Defined User Roles Setup** (Configuration des rôles d'utilisateur définis par ASDM) s'affiche. Cliquez sur **Yes** (Oui) pour utiliser les privilèges de compte d'utilisateur prédéfinis : **Admin** (niveau de privilège 15, avec accès complet à toutes les commandes de l'interface de ligne de commande); **Lecture seule** (niveau de privilège 5, avec accès en lecture seule); et **Affichage unquement** (niveau de privilège 3, avec accès à la section **de surveillance** seulement).

- Cliquez sur **Configure Command Privileges** (Configurer les privilèges de commande) pour configurer manuellement les niveaux de commande.

  La boîte de dialogue **Command Privileges Setup** (Configuration des privilèges de commande) apparaît. Vous pouvez afficher toutes les commandes en sélectionnant **All Modes** (Tous les modes) dans la liste déroulante **Command Mode** (Mode de commande), ou vous pouvez choisir un mode de configuration pour afficher les commandes disponibles dans ce mode. Par exemple, si vous choisissez contexte, vous pouvez afficher toutes les commandes disponibles en mode de configuration de contexte. Si une commande peut être saisie en mode EXEC de l'utilisateur ou en mode d'exécution privilégié ainsi qu'en mode de configuration et que la commande effectue des actions différentes dans chaque mode, vous pouvez définir le niveau de privilège pour ces modes séparément.

  La colonne **Variant** (Variante) affiche show, clear ou cmd. Vous pouvez définir les privilèges uniquement pour la forme show, clear ou configure de la commande. La forme configure de la commande est généralement la forme qui entraîne une modification de configuration, soit sous forme de commande non modifiée (sans le préfixe show ou clear), soit sous forme no (non).

  Pour modifier le niveau d'une commande, double-cliquez dessus ou cliquez sur **Edit** (Modifier). Vous pouvez définir le niveau entre 0 et 15. Vous pouvez uniquement configurer le niveau de privilège de la commande principale. Par exemple, vous pouvez configurer le niveau de toutes les commandes **aaa**, mais pas le niveau des commandes **aaa authentication** et **aaa authorization** séparément.

  Pour modifier le niveau de toutes les commandes qui s'affichent, cliquez sur **Select All** (Sélectionner tout), puis sur **Edit** (Modifier).

  Cliquez sur **OK** pour accepter vos modifications.

Étape 5 (Facultatif) Cochez la case **Perform authorization for exec shell access (Effectuer l'autorisation pour l'accès au shell d'exécution)** > **Enable (Activer)** afin d'activer les utilisateurs AAA pour l'autorisation de commande. Sans cette option, l'ASA ne prend en charge que les niveaux de privilège des utilisateurs de base de données locaux et définit par défaut tous les autres types d'utilisateurs au niveau 15.

Cette commande active également l'autorisation de gestion. Consultez Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion, à la page 24.

Étape 6 Cliquez sur **Apply** (Appliquer).

Les paramètres d'autorisation sont affectés et les modifications sont enregistrées dans la configuration en cours d'exécution.

Configurer les commandes sur le serveur TACACS+

Vous pouvez configurer des commandes sur un serveur TACACS+ Cisco Secure Access Control Server (ACS) en tant que composant de profil partagé, pour un groupe ou pour des utilisateurs individuels. Pour les serveurs TACACS+ tiers, consultez la documentation de votre serveur pour en savoir plus sur la prise en charge des autorisations de commandes.

Consultez les lignes directrices suivantes pour la configuration des commandes dans Cisco Secure ACS version 3.1; la plupart de ces lignes directrices s'appliquent également aux serveurs tiers :

- L'ASA envoie les commandes à autoriser en tant que commandes shell; veuillez donc configurer les commandes sur le serveur TACACS+ en tant que commandes shell.

Remarque Cisco Secure ACS peut inclure un type de commande appelé « pix-shell ». N'utilisez pas ce type pour l'autorisation de commande ASA.

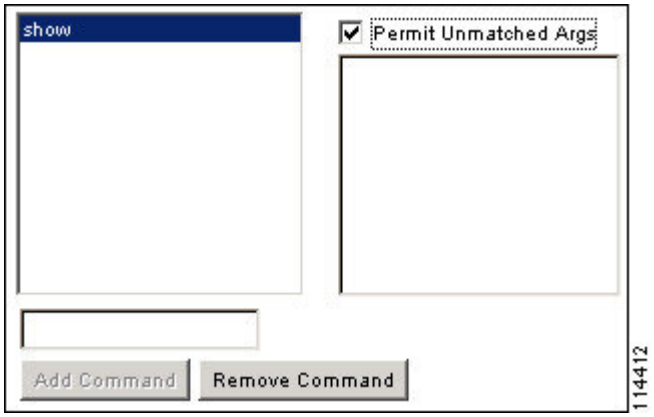
- Le premier mot de la commande est considéré comme la commande principale. Tous les mots supplémentaires sont considérés comme des arguments, qui doivent être précédés de **permit** ou **deny**.

  Par exemple, pour autoriser la commande **show running-configuration aaa-server**, ajoutez **show running-configuration** dans le champ de la commande et saisissez **permit aaa-server** dans le champ des arguments.

- Vous pouvez autoriser tous les arguments d'une commande que vous ne refusez pas explicitement en cochant la case **Permit Unmatched Args** (Autoriser les arguments sans correspondance).

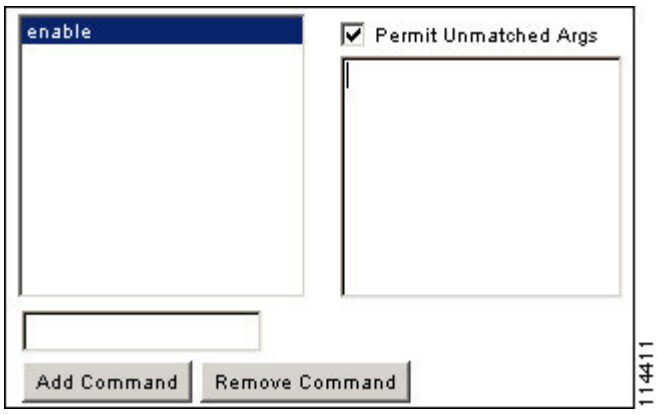
  Par exemple, vous pouvez configurer uniquement la commande **show**. Toutes les commandes **show** sont autorisées. Nous vous conseillons d'utiliser cette méthode pour que vous n'ayez pas à anticiper chaque variante d'une commande, y compris les abréviations et un point d'interrogation, qui indique l'utilisation de l'interface de ligne de commande (voir la figure suivante).

Illustration 1 : Autoriser toutes les commandes associées



- Pour les commandes composées d'un seul mot, vous *devez* autoriser des arguments sans correspondance, même s'il n'y a aucun argument pour la commande, par exemple **enable** ou **help** (voir la figure suivante).

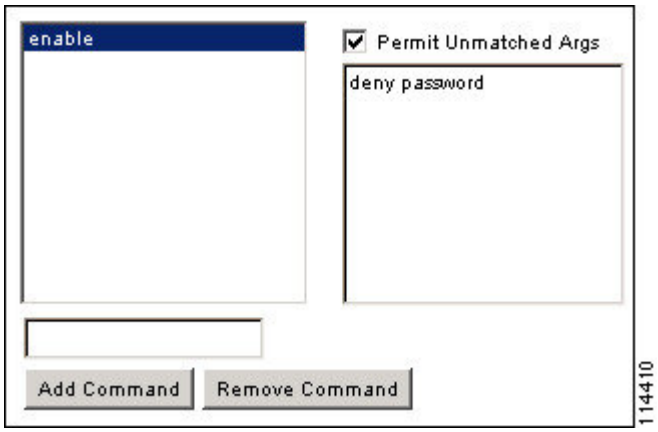
Illustration 2 : Autorisation des commandes à un seul mot



- Pour interdire certains arguments, entrez les arguments précédés de **deny**.

  Par exemple, pour autoriser **enable**, mais pas **enable password**, saisissez **enable** dans le champ des commandes et **deny password** dans le champ des arguments. Assurez-vous de cocher la case **Permit Unmatched Args** (Autoriser les arguments sans correspondance) pour que **enable** soit toujours autorisé (voir la figure suivante).

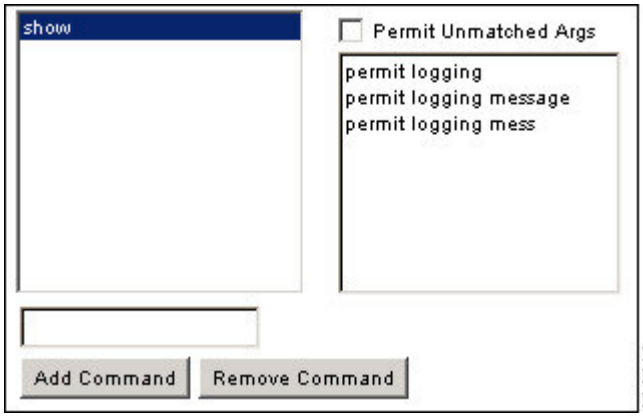
Illustration 3 : Interdire les arguments



- Lorsque vous abrégez une commande dans la ligne de commande, l'ASA développe le préfixe et la commande principale en texte intégral, mais envoie des arguments supplémentaires au serveur TACACS+ au fur et à mesure que vous les saisissez.

  Par exemple, si vous saisissez **sh log**, l'ASA envoie la commande complète au serveur TACACS+, **show logging**. Cependant, si vous saisissez **sh log mess**, l'ASA envoie **show logging mess** au serveur TACACS+, et non la commande étendue **show logging message**. Vous pouvez configurer plusieurs orthographes du même argument afin d'anticiper les abréviations (voir la figure suivante).

Illustration 4 : Spécifier les abréviations



- Nous vous conseillons d'autoriser les commandes de base suivantes pour tous les utilisateurs :
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**
  - **clear pager**
  - **quit**
  - **show version**

Configurer l'autorisation de commande TACACS+

Si vous activez l'autorisation de commande TACACS+ et qu'un utilisateur saisit une commande au niveau de l'interface de ligne de commande, l'ASA envoie la commande et le nom d'utilisateur au serveur TACACS+ pour déterminer si la commande est autorisée.

Avant d'activer l'autorisation de commande TACACS+, assurez-vous d'être connecté à l'ASA en tant qu'utilisateur défini sur le serveur TACACS+ et de disposer de l'autorisation de commande nécessaire pour continuer à configurer l'ASA. Par exemple, vous devez vous connecter en tant qu'utilisateur admin avec toutes les commandes autorisées. Sinon, vous pourriez vous retrouver involontairement bloqué.

N'enregistrez pas votre configuration avant d'être sûr qu'elle fonctionne comme vous le souhaitez. Si vous êtes bloqué par erreur, vous pouvez généralement récupérer l'accès en redémarrant l'ASA.

Assurez-vous que votre système TACACS+ est complètement stable et fiable. Le niveau de fiabilité nécessaire exige généralement que vous ayez un système de serveurs TACACS+ entièrement redondant et une connectivité entièrement redondante à l'ASA. Par exemple, dans votre ensemble de serveurs TACACS+, incluez un serveur connecté à l'interface 1 et un autre à l'interface 2. Vous pouvez également configurer l'autorisation de commande locale comme méthode de secours si le serveur TACACS+ n'est pas disponible.

Pour configurer l'autorisation de commande à l'aide d'un serveur TACACS+, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)**

Étape 2 Cochez la case **Enable authorization for command access (Activer l'autorisation pour l'accès à la commande)** > **Enable (Activer)**.

Étape 3 Choisissez un nom de groupe de serveurs AAA dans la liste déroulante **Server Group** (Groupe de serveurs).

Étape 4 (Facultatif) Vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Pour ce faire, cochez la case **Use LOCAL when server group fails** (Utiliser LOCAL en cas d'échec du groupe de serveurs). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée. Assurez-vous de configurer les utilisateurs dans la base de données locale et les niveaux de privilège de commande.

Étape 5 Cliquez sur **Apply** (Appliquer).

Les paramètres d'autorisation de commande sont affectés et les modifications sont enregistrées dans la configuration d'exécution.

Configurer une politique de mot de passe pour les utilisateurs de base de données locale

Lorsque vous configurez l'authentification pour l'accès à l'interface de ligne de commande ou à ASDM à l'aide de la base de données locale, vous pouvez configurer une politique de mot de passe qui oblige un utilisateur à changer de mot de passe après une durée spécifiée et qui exige également des normes de mot de passe tel qu'une longueur minimum et le nombre minimum de modifications de caractères.

La politique de mot de passe s'applique uniquement aux utilisateurs administratifs qui utilisent la base de données locale et non aux autres types de trafic qui peuvent utiliser la base de données locale, comme le VPN ou l'AAA pour l'accès au réseau, et non aux utilisateurs authentifiés par un serveur AAA.

Après avoir configuré la politique de mot de passe, lorsque vous modifiez un mot de passe (le vôtre ou celui d'un autre utilisateur), la politique de mot de passe s'applique au nouveau mot de passe. Tous les mots de passe existants sont conservés. La nouvelle politique s'applique à la modification du mot de passe avec la le volet **User Accounts** (Comptes d'utilisateurs) et la le volet **Change My Password** (Changer mon mot de passe).

Avant de commencer

- Configurez l'authentification AAA pour l'accès de l'interface de ligne de commande ou ASDM à l'aide de la base de données locale.
- Spécifiez les noms d'utilisateurs dans la base de données locale.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Password Policy (Politique de mot de passe)**.

Étape 2 Configurez n'importe quelle combinaison des options suivantes :

- **Minimum Password Length** (Longueur minimum du motde passe) : saisissez la longueur minimum des mots de passe. Les valeurs valides sont comprises entre 3 et 64 caractères. La longueur minimum conseillée du mot de passe est de 8 caractères.
- **Lifetime** (Durée de vie) : saisissez l'intervalle en jours après lequel les mots de passe expirent pour les utilisateurs distants (SSH, Telnet, HTTP); les utilisateurs au niveau du port de console ne sont jamais verrouillés en raison de l'expiration du mot de passe. Les valeurs valides sont comprises entre 0 et 65536 jours. La valeur par défaut est 0 jour, une valeur indiquant que les mots de passe n'expireront jamais.

  7 jours avant l'expiration du mot de passe, un message d'avertissement s'affiche. À l'expiration du mot de passe, l'accès au système est refusé aux utilisateurs distants. Pour y accéder après l'expiration, effectuez l'une des opérations suivantes :

  - Demandez à un autre administrateur de modifier votre mot de passe.
  - Connectez-vous au port de console physique pour modifier votre mot de passe.

- **Minimum Number Of** (Nombre minimum de) : spécifiez le nombre minimum de caractères parmi les types suivants :
  - **Numeric Characters** (Caractères numériques) : saisissez le nombre minimum de caractères numériques que les mots de passe doivent contenir. Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0.
  - **Lower Case Characters** (Caractères minuscules) : saisissez le nombre minimum de caractères minuscules que les mots de passe doivent contenir. Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0.
  - **Upper Case Characters** (Caractères majuscules) : saisissez le nombre minimum de caractères majuscules que les mots de passe doivent contenir. Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0.
  - **Special Characters** (Caractères spéciaux) : saisissez le nombre minimum de caractères spéciaux que les mots de passe doivent contenir. Les valeurs valides sont comprises entre 0 et 64 caractères. Les caractères spéciaux sont les suivants : !, @, #, $, %, ^, &, *, « (» et «) ». La valeur par défaut est 0.
  - **Different Characters from Previous Password** (Caractères différents du mot de passe précédent) : saisissez le nombre minimum de caractères que vous devez modifier entre l'ancien et le nouveau mot de passe. Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est

0. La correspondance des caractères est indépendante de la position, ce qui signifie que les caractères du nouveau mot de passe ne sont considérés comme modifiés que s'ils n'apparaissent nulle part dans le mot de passe actuel.

- **Enable Reuse Interval** (Activer l'intervalle de réutilisation) : vous pouvez interdire la réutilisation d'un mot de passe correspondant aux mots de passe utilisés précédemment, entre 2 et 7 mots de passe précédents. Les mots de passe précédents sont stockés dans la configuration sous chaque nom d'utilisateur sous forme chiffrée à l'aide de la commande **password-history**; cette commande n'est pas configurable par l'utilisateur.
- **Prevent Passwords from Matching Usernames** (Empêcher les mots de passe de correspondre aux noms d'utilisateurs) : interdisez un mot de passe qui correspond à un nom d'utilisateur.

Étape 3 (Facultatif) Cochez la case **Enable Password and Account Protection** (Activer la protection du mot de passe et du compte) pour demander aux utilisateurs de changer de mot de passe dans le volet **Change My Password** (Changer mon mot de passe) au lieu du volet **User Accounts** (Comptes d'utilisateurs). Le paramètre par défaut est désactivé : un utilisateur peut utiliser l'une ou l'autre des méthodes pour modifier son mot de passe.

Si vous activez cette fonctionnalité et essayez de changer votre mot de passe dans le volet **User Accounts** (Comptes d'utilisateurs), le message d'erreur suivant est généré :

```
ERROR: Changing your own password is prohibited
```

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer les paramètres de configuration.

Changer votre mot de passe

Si vous configurez une durée de validité du mot de passe dans la politique de mot de passe, vous devez changer votre mot de passe lorsque l'ancien mot de passe expire. Cette méthode de modification du mot de passe est requise si vous activez l'authentification par politique de mot de passe. Si l'authentification par politique de mot de passe n'est pas activée, vous pouvez utiliser cette méthode ou vous pouvez modifier directement votre compte d'utilisateur.

Pour modifier votre mot de passe d'utilisateur, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Change Password (Modifier le mot de passe)**.

Étape 2 Saisissez votre ancien mot de passe.

Étape 3 Saisissez votre nouveau mot de passe.

Étape 4 Confirmez votre nouveau mot de passe.

Étape 5 Cliquez sur **Make Change** (Appliquer la modification).

Étape 6 Cliquez sur l'icône **Save** (Enregistrer) pour enregistrer vos modifications dans la configuration en cours d'exécution.

Activer et afficher l'historique de connexion

Par défaut, l'historique de connexion est enregistré pendant 90 jours. Vous pouvez désactiver cette fonctionnalité ou modifier la durée, jusqu'à 365 jours.

Avant de commencer

- L'historique de connexion n'est enregistré que par unité; dans les environnements de basculement et de mise en grappe, chaque unité conserve uniquement son propre historique de connexion.
- Les données de l'historique de connexion ne sont pas conservées pendant les rechargements.
- Cette fonctionnalité s'applique aux noms d'utilisateur dans la base de données locale ou à partir d'un serveur AAA lorsque vous activez l'authentification AAA locale pour une ou plusieurs des méthodes de gestion de l'interface de ligne de commande (SSH, Telnet, console série). Les connexions à ASDM ne sont pas enregistrées dans l'historique.

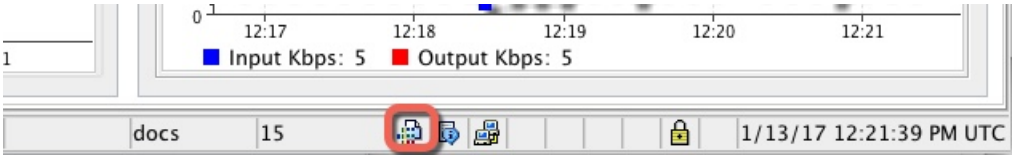
Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Login History (Historique de connexion)**.

Étape 2 Cochez la case **Configure login history reporting for administrators** (Configurer les rapports d'historique de connexion pour les administrateurs). Cette fonction est activée par défaut.

Étape 3 Définissez la **durée** entre 1 et 365 jours. La valeur par défaut est 90.

Étape 4 Pour afficher l'historique de connexion, à partir de n'importe quel écran ASDM, vous pouvez cliquer sur l'icône **Login History** (Historique de connexion) dans la barre **Status** (État) inférieure :



L'historique de connexion de tous les utilisateurs s'affiche dans une boîte de dialogue.

Configurer la traçabilité de l'accès de gestion

Vous pouvez envoyer des messages de traçabilité au serveur de comptabilité TACACS+ lorsque vous saisissez une commande autre que les commandes **show** au niveau de l'interface de ligne de commande. Vous pouvez configurer la comptabilisation lorsque les utilisateurs se connectent, lorsqu'ils saisissent la commande **enable** ou lorsqu'ils émettent des commandes.

Pour la traçabilité des commandes, vous pouvez uniquement utiliser des serveurs TACACS+.

Pour configurer l'accès de gestion et activer la traçabilité des commandes, procédez comme suit :

Procédure

Étape 1 Pour activer la comptabilisation des utilisateurs lorsqu'ils saisissent la commande **enable**, procédez comme suit :

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Accounting (Traçabilité)**, puis cochez la case **Require accounting to allow accounting of user activity (Exiger la traçabilité pour permettre la comptabilisation de l'activité de l'utilisateur)** > **Enable (Activer)**.

b) Choisissez un nom de groupe de serveurs RADIUS ou TACACS+.

Étape 2 Pour activer la comptabilisation des utilisateurs lorsqu'ils accèdent à l'ASA à l'aide de Telnet, de SSH ou de la console de série, procédez comme suit :

a) Cochez les cases **Serial** (Série), **SSH** et/ou **Telnet** dans la zone **Require accounting for the following types of connections** (Exiger la traçabilité pour les types de connexions suivants).

b) Choisissez un nom de groupe de serveurs RADIUS ou TACACS+ pour chaque type de connexion.

Étape 3 Pour configurer la traçabilité des commandes, procédez comme suit :

a) Cochez la case **Enable** (Activer) dans la zone **Require accounting for the following types of connections** (Exiger la traçabilité pour les types de connexions suivants).

b) Choisissez un nom de groupe de serveurs TACACS+. RADIUS n'est pas pris en charge.

Vous pouvez envoyer des messages de traçabilité au serveur de comptabilité TACACS+ lorsque vous saisissez une commande autre que les commandes **show** au niveau de l'interface de ligne de commande.

c) Si vous personnalisez le niveau de privilège des commandes à l'aide de la boîte de dialogue **Command Privilege Setup** (Configuration des privilèges de commande), vous pouvez limiter les commandes pour lesquelles l'ASA est responsable en précisant un niveau de privilège minimum dans la liste déroulante **Privilege level** (Niveau de privilège). L'ASA ne prend pas en compte les commandes dont le niveau de privilège est inférieur.

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

Les paramètres de comptabilisation sont affectés et les modifications sont enregistrées dans la configuration d'exécution.

Récupérer d'un verrouillage

Dans certaines circonstances, lorsque vous activez l'autorisation de commande ou l'authentification de l'interface de ligne de commande, vous pouvez être verrouillé hors de l'interface de ligne de commande de l'ASA. Vous pouvez généralement récupérer l'accès en redémarrant l'ASA. Cependant, si vous avez déjà enregistré votre configuration, vous pourriez être verrouillé.

Le tableau suivant répertorie les conditions de verrouillage courantes et la façon dont vous pouvez y remédier.

Tableau 1 : Scénarios de verrouillage de l'authentification de l'interface de ligne de commande et de l'autorisation de commande

Fonctionnalités	Condition de verrouillage	Description	Solution de contournement : mode unique	Solution de contournement : mode multiple
Authentification de l'interface de ligne de commande locale	Aucun utilisateur n'a été configuré dans la base de données locale.	Si vous n'avez aucun utilisateur dans la base de données locale, vous ne pouvez pas vous connecter ni ajouter d'utilisateurs.	Connectez-vous et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et ajouter un utilisateur.
Autorisation de commande TACACS+ Authentification de l'interface de ligne de commande TACACS+ Authentification de l'interface de ligne de commande RADIUS	Le serveur est en panne ou inaccessible et vous n'avez pas configuré la méthode de secours.	Si le serveur est inaccessible, vous ne pouvez pas vous connecter ni saisir de commandes.	**1.** Connectez-vous et réinitialisez les mots de passe et les commandes AAA. **2.** Configurez la base de données locale comme méthode de secours afin de ne pas être verrouillé lorsque le serveur est en panne.	**1.** Si le serveur est inaccessible en raison d'une configuration de réseau incorrecte sur l'ASA, connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et reconfigurer vos paramètres réseau. **2.** Configurez la base de données locale comme méthode de secours afin de ne pas être verrouillé lorsque le serveur est en panne.
Autorisation de commande TACACS+	Vous êtes connecté en tant qu'utilisateur sans privilèges suffisants ou en tant qu'utilisateur qui n'existe pas.	Vous activez l'autorisation de commande, mais vous constatez ensuite que l'utilisateur ne peut plus saisir de commandes.	Corrigez le compte d'utilisateur du serveur TACACS+. Si vous n'avez pas accès au serveur TACACS+ et que vous devez configurer l'ASA immédiatement, connectez-vous à la partition de maintenance et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et terminer les modifications de configuration. Vous pouvez également désactiver l'autorisation de commande jusqu'à ce que vous corrigiez la configuration TACACS+.
Autorisation de commande locale	Vous êtes connecté en tant qu'utilisateur sans privilèges suffisants.	Vous activez l'autorisation de commande, mais vous constatez ensuite que l'utilisateur ne peut plus saisir de commandes.	Connectez-vous et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et changer le niveau d'utilisateur.

Accès au moniteur

- **Monitoring (Supervision)** > **Properties (Propriétés)** > **Device Access (Accès au périphérique)** > **ASDM/HTTPS/Telnet/SSH Sessions (Sessions ASDM/HTTPS/Telnet/SSH)**

  Le volet supérieur répertorie les types de connexion, les ID de session et les adresses IP des utilisateurs connectés par le biais des sessions ASDM, HTTPS et Telnet. Pour déconnecter une session en particulier, cliquez sur **Disconnect** (Déconnecter).

  Le volet inférieur répertorie les clients, les noms d'utilisateur, les états de connexion, les versions logicielles, les types de chiffrement entrants, les types de chiffrement sortants, les HMAC entrants, les HMAC sortants, les ID de session SSH, les données de renouvellement restantes, le temps de renouvellement restant, les renouvellements basés sur les données, les renouvellements basés sur le temps et l'heure de la dernière reconnexion. Pour déconnecter une session en particulier, cliquez sur **Disconnect** (Déconnecter).

- **Monitoring (Supervision)** > **Properties (Propriétés)** > **Device Access (Accès au périphérique)** > **Authenticated Users (Utilisateurs authentifiés)**

  Ce volet répertorie les noms d'utilisateur, les adresses IP, les listes de contrôle d'accès dynamique, les délais d'inactivité (le cas échéant) et les délais absolus des utilisateurs qui ont été authentifiés par les serveurs AAA.

- **Monitoring (Supervision)** > **Properties (Propriétés)** > **Device Access (Accès au périphérique)** > **AAA Locked Out Users (Utilisateurs AAA verrouillés)**

  Ce volet répertorie les noms d'utilisateur des utilisateurs locaux AAA verrouillés, le nombre de tentatives d'authentification en échec et les heures auxquelles les utilisateurs ont été verrouillés. Pour effacer un utilisateur spécifique qui a été verrouillé, cliquez sur **Clear Selected Lockout** (Effacer le verrouillage sélectionné). Pour effacer tous les utilisateurs qui ont été verrouillés, cliquez sur **Clear All Lockouts** (Effacer tous les verrouillages).

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique de l'accès de gestion

Tableau 2 : Historique de l'accès de gestion

Nom de la caractéristique	Versions de plateforme	Description
Pile CiscoSSH maintenant par défaut	9.19(1)	La pile Cisco SSH est maintenant utilisée par défaut. Écrans Nouveaux ou modifiés : • Mode de contexte unique : **Configuration** > **Device Management (Gestion des appareils)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** • Mode de contexte multiple : **Configuration** > **Device Management (Gestion des appareils)** > **SSH Stack (Pile SSH)**

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de l'interface de boucle avec retour pour SSH et Telnet	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour les fonctionnalités suivantes : • SSH • Telnet Commandes nouvelles/modifiées : **interface loopback**, **ssh**, **telnet** Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**. La prise en charge d'ASDM a été ajoutée dans la version 7.19.
Pile CiscoSSH	9.17(1)	L'ASA utilise une pile SSH propriétaire pour les connexions SSH. Vous pouvez maintenant choisir d'utiliser à la place la pile CiscoSSH, qui est basée sur OpenSSH. La pile par défaut continue d'être la pile ASA. Cisco SSH prend en charge : • Conformité FIPS • Mises à jour régulières, y compris les mises à jour de Cisco et de la communauté de code source libre. Notez que la pile CiscoSSH ne prend pas en charge : • SSH vers une interface différente sur VPN (accès de gestion) • Paire de clés EdDSA • Paire de clés RSA en mode FIPS Si vous avez besoin de ces fonctionnalités, vous devez continuer à utiliser la pile SSH ASA. Il y a une petite modification de la fonctionnalité SCP avec la pile CiscoSSH : pour utiliser la commande **copy** de l'ASA pour copier un fichier vers ou à partir d'un serveur SCP, vous devez activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP. Écrans Nouveaux ou modifiés : • Mode de contexte unique : **Configuration** > **Device Management (Gestion des appareils)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** • Mode de contexte multiple : **Configuration** > **Device Management (Gestion des appareils)** > **SSH Stack (Pile SSH)**

Nom de la caractéristique	Versions de plateforme	Description
Modifications du verrouillage de l'utilisateur local	9.17(1)	L'ASA peut verrouiller les utilisateurs locaux après un nombre configurable de tentatives de connexion échouées. Cette fonctionnalité ne s'applique pas aux utilisateurs ayant le niveau de privilège 15. De plus, un utilisateur serait verrouillé indéfiniment jusqu'à ce qu'un administrateur déverrouille son compte. Désormais, les utilisateurs seront déverrouillés après 10 minutes, à moins qu'un administrateur n'utilise la commande **clear aaa local user lockout** avant. Les utilisateurs ayant le niveau de privilège 15 sont également concernés par le paramètre de verrouillage. Commandes nouvelles ou modifiées : **aaa local authentication attempts max-fail** , **show aaa local user**
Invite de modification du mot de passe SSH et Telnet	9.17(1)	La première fois qu'un utilisateur local se connecte à l'ASA à l'aide de SSH ou de Telnet, il est invité à changer de mot de passe. Il sera également invité à se connecter pour la première fois après qu'un administrateur aura modifié son mot de passe. Si l'ASA se recharge, les utilisateurs ne seront pas invités, même s'il s'agit de leur première connexion. Notez que tout service qui utilise la base de données des utilisateurs locale, comme VPN, devra également utiliser le nouveau mot de passe s'il a été modifié lors d'une connexion SSH ou Telnet. Commandes nouvelles ou modifiées : **show aaa local user**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de la sécurité SSH	9.16(1)	SSH prend désormais en charge les améliorations de sécurité suivantes : • Format de clé d'hôte : **crypto key generate** {**eddsa** | **ecdsa**}. En plus de RSA, nous avons ajouté la prise en charge des clés d'hôte EdDSA et ECDSA. L'ASA essaie d'utiliser les clés dans l'ordre suivant, si elles existent : EdDSA, ECDSAA, puis RSA. 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. • Algorithmes d'échange de clés : **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • Algorithmes de chiffrement : **ssh cipher encryption chacha20-poly1305@openssh.com** • La version 1 de SSH n'est plus prise en charge. La commande **ssh version** est supprimée. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** • **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)** • **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)**
Accès de gestion pour SNMP	9.14(2)	Lors de la configuration de l'accès de gestion sur un tunnel VPN, incluez l'adresse IP de l'interface externe dans la liste d'accès de la carte cryptographique dans le cadre de la configuration du VPN pour sécuriser l'interrogation SNMP sur un VPN de site à site.

Nom de la caractéristique	Versions de plateforme	Description
Paramètre de délai d'inactivité HTTPS	9.14(1)	Vous pouvez maintenant définir le délai d'inactivité pour toutes les connexions HTTPS à l'ASA, y compris ASDM, WebVPN et d'autres clients. Auparavant, avec la commande **http server idle-timeout**, vous pouviez uniquement définir le délai d'inactivité d'ASDM. Si vous définissez les deux délais, la nouvelle commande prévaut. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** > **HTTP Settings (Paramètres HTTP)** > **case Connection Idle Timeout (Délai d'inactivité de la connexion)**.
Le chiffrement SSH est désormais répertorié (de la sécurité la plus haute à la plus basse) pour les listes prédéfinies	9.13(1)	Le chiffrement SSH est désormais répertorié (de la sécurité la plus haute à la sécurité la plus basse) pour les listes prédéfinies (comme moyen ou élevé). Dans les versions précédentes, il était répertorié du niveau le plus bas au plus élevé, ce qui signifie qu'un chiffrement à faible sécurité serait proposé avant un chiffrement à sécurité élevée. Écrans Nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)**
La définition du mode d'échange de clés SSH est limitée au contexte d'administration	9.12(2)	Vous devez définir l'échange de clés SSH dans le contexte d'administration; ce paramètre est hérité par tous les autres contextes. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** > **SSH Settings (Paramètres SSH)** > **DH Key Exchange (Échange de clés DH)**
Le changement de mot de passe **enable** est maintenant requis lors de la connexion	9.12(1)	Le mot de passe par défaut **enable** est vide. Lorsque vous essayez d'accéder en mode d'exécution privilégié sur l'ASA, vous devez désormais modifier le mot de passe pour une valeur de 3 caractères ou plus. Vous ne pouvez pas le garder vide. La commande **no enable password** n'est plus prise en charge. Au niveau de l'interface de ligne de commande, vous pouvez accéder au mode d'exécution privilégié à l'aide des commandes **enable**, **login** (avec un utilisateur de niveau de privilège 2+), ou d'une session SSH ou Telnet lorsque vous activez **aaa authorization exec auto-enable**. Toutes ces méthodes nécessitent que vous définissiez le mot de passe d'activation. Cette exigence de changement de mot de passe n'est pas appliquée pour les connexions ASDM. Dans ASDM, par défaut, vous pouvez vous connecter sans nom d'utilisateur et avec le mot de passe **enable**. Aucun écran modifié.

Nom de la caractéristique	Versions de plateforme	Description
Limitation configurable des sessions d'administration	9.12(1)	Vous pouvez configurer le nombre maximum de sessions administratives agrégées, par utilisateur et par protocole. Auparavant, vous pouviez configurer uniquement le nombre agrégé de sessions. Cette fonctionnalité n'influe pas sur les sessions de console. Notez qu'en mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions HTTPS, où le maximum est fixé à 5 sessions. La commande **quota management-session** n'est également plus acceptée dans la configuration système et est plutôt disponible dans la configuration du contexte. Le nombre maximum de sessions agrégées est désormais de 15; si vous avez configuré 0 (illimité) ou 16+, lors de la mise à niveau, la valeur passe à 15. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Management Session Quota (Quota de sessions de gestion)**
Notifications pour les modifications du niveau de privilège d'administration	9.12(1)	Lorsque vous vous authentifiez pour activer l'accès (**aaa authentication enable console**) ou autorisez directement l'accès EXEC privilégié (**aaa authorization exec auto-enable**), l'ASA informe désormais les utilisateurs si le niveau d'accès qui leur a été attribué a changé depuis leur dernière connexion. Écrans Nouveaux ou modifiés : Barre **Status (État)** > icône **Login History (Historique de connexion)**
Sécurité SSH renforcée	9.12(1)	Consultez les améliorations de sécurité SSH suivantes : • Prise en charge de l'échange de clés SHA256, groupe Diffie-Hellman 14. Ce paramètre est désormais la valeur par défaut. L'ancienne valeur par défaut était le groupe 1 SHA1. • Prise en charge du chiffrement d'intégrité HMAC-SHA256. La valeur par défaut est désormais l'ensemble de chiffrements à haute sécurité (hmac-sha2-256 uniquement). L'ancienne valeur par défaut était l'ensemble moyen. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** • **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffrement SSH)**

Nom de la caractéristique	Versions de plateforme	Description
Autoriser les clients HTTPS non basés sur le navigateur à accéder à l'ASA	9.12(1)	Vous pouvez autoriser les clients HTTPS non basés sur le navigateur à accéder aux services HTTPS sur l'ASA. Par défaut, ASDM, CSM et l'API REST sont autorisés. Écrans nouveaux ou modifiés. **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **HTTP Non-Browser Client Support (Prise en charge des clients HTTP non basés sur le navigateur)**
La paire de clés RSA prend en charge les clés de 3 072 bits	9.9(2)	Vous pouvez maintenant définir la taille du module à 3 072. Écran nouveau ou modifié : **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**
Accès de gestion du VPN sur les interfaces virtuelles pontées (BVI)	9.9(2)	Vous pouvez maintenant activer des services de gestion, tels que **telnet**, **http** et **ssh**, sur une BVI si le paramètre **management-access** du VPN a été activé sur cette BVI. Pour l'accès de gestion non VPN, vous devez continuer à configurer ces services sur les interfaces membres du groupe de ponts. Commandes nouvelles ou modifiées : **https**, **telnet**, **ssh**, **management-access**
La version 1 de SSH est obsolète	9.9(1)	La version 1 de SSH est obsolète et sera supprimée dans une version ultérieure. Le paramètre par défaut est passé de SSH v1 et v2 à SSH v2. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**

Nom de la caractéristique	Versions de plateforme	Description
Authentification distincte pour les utilisateurs disposant d'une authentification par clé publique SSH et les utilisateurs disposant de mots de passe	9.6(3)/9.8(1)	Dans les versions antérieures à 9.6(2), vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer explicitement l'authentification SSH AAA avec la base de données des utilisateurs locale (**aaa authentication ssh console LOCAL**). Dans 9.6(2), l'ASA vous a demandé d'activer explicitement l'authentification SSH AAA. Dans cette version, vous n'avez plus à activer explicitement l'authentification SSH AAA; lorsque vous configurez la commande **ssh authentication** pour un utilisateur, l'authentification locale est activée par défaut pour les utilisateurs avec ce type d'authentification. De plus, lorsque vous configurez explicitement l'authentification SSH AAA, cette configuration s'applique uniquement aux noms d'utilisateur avec *mots de passe*, et vous pouvez utiliser n'importe quel type de serveur AAA (**aaa authentication ssh console radius_1**, par exemple). Par exemple, certains utilisateurs peuvent utiliser l'authentification par clé publique à l'aide de la base de données locale et d'autres utilisateurs peuvent utiliser des mots de passe avec RADIUS. Nous n'avons pas modifié d'écrans.
Historique de connexion	9.8(1)	Par défaut, l'historique de connexion est enregistré pendant 90 jours. Vous pouvez désactiver cette fonctionnalité ou modifier la durée, jusqu'à 365 jours. Cette fonctionnalité s'applique uniquement aux noms d'utilisateur dans la base de données locale lorsque vous activez l'authentification AAA locale pour une ou plusieurs des méthodes de gestion (SSH, ASDM, Telnet, etc.). Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Login History (Historique de connexion)**
Application de la politique de mot de passe pour interdire la réutilisation des mots de passe et l'utilisation d'un mot de passe correspondant à un nom d'utilisateur	9.8(1)	Vous pouvez désormais interdire la réutilisation des mots de passe précédents pour un maximum de 7 générations, et vous pouvez également interdire l'utilisation d'un mot de passe correspondant à un nom d'utilisateur. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Password Policy (Politique de mot de passe)**
Mode du serveur SSL ASA correspondant à ASDM	9.6(2)	Pour un utilisateur ASDM qui s'authentifie avec un certificat, vous pouvez désormais exiger que le certificat corresponde à une carte de certificat. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de l'authentification par clé publique SSH	9.6(2)	Dans les versions antérieures, vous pouviez activer l'authentification par clé publique SSH sans activer également l'authentification SSH AAA avec la base de données d'utilisateurs locale . La configuration est désormais modifiée de manière à ce que vous deviez explicitement activer l'authentification SSH AAA. Pour empêcher les utilisateurs d'utiliser un mot de passe au lieu de la clé privée, vous pouvez désormais créer un nom d'utilisateur sans mot de passe défini. Nous avons modifié les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)**
Autorisation de gestion ASDM	9.4(1)	Vous pouvez désormais configurer l'autorisation de gestion séparément pour l'accès HTTP par rapport à l'accès Telnet et SSH. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Autorisation)**
Nom d'utilisateur ASDM dans la configuration du certificat	9.4(1)	Lorsque vous activez l'authentification par certificat ASDM, vous pouvez configurer la façon dont ASDM extrait le nom d'utilisateur du certificat; vous pouvez également activer le préremplissage du nom d'utilisateur à l'invite de connexion. Nous avons introduit l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > HTTP Certificate Rule (Règle de certificat HTTP).**
Authentification par mot de passe à usage unique améliorée	9.2(1)	Les administrateurs qui disposent de privilèges d'autorisation suffisants peuvent passer en mode d'exécution privilégié en saisissant une seule fois leurs informations d'authentification. L'option **auto-enable** a été ajoutée à la commande **aaa authorization exec**. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authorization (Autorisation).
Prise en charge de la redirection HTTP pour IPV6	9.1(7)/9.6(1)	Lorsque vous activez la redirection HTTP vers HTTPS pour l'accès ASDM ou le SSL VPN sans client, vous pouvez désormais rediriger le trafic envoyé par vers l'adresse IPv6. Nous avons ajouté des fonctionnalités à l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **HTTP Redirect (Redirection HTTP)**

Nom de la caractéristique	Versions de plateforme	Description
Chiffrement SSH et d'intégrité configurables	9.1(7.4), 9.5(3), 9.6(1)	Les utilisateurs peuvent sélectionner des modes de chiffrement lors de la gestion du chiffrement SSH et peuvent configurer le HMAC et le chiffrement pour divers algorithmes d'échange de clés. Vous souhaiterez peut-être modifier les chiffres pour qu'ils soient plus ou moins stricts, selon votre application. Notez que la performance de la copie sécurisée dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier les chiffres proposés, utilisez **ssh cipher encryption custom aes128-cbc**, par exemple. Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSH Ciphers (Chiffres SSH)**
Chiffrement AES-CTR pour SSH	9.1(2)	La mise en œuvre du serveur SSH dans l'ASA prend désormais en charge le chiffrement en mode AES-CTR.
Intervalle de renouvellement SSH amélioré	9.1(2)	Une connexion SSH est renouvelée après 60 minutes de connexion ou 1 Go de trafic de données. .
Pour l'ASASM en mode de contexte multiple, prenez en charge l'authentification Telnet et de la console virtuelle à partir du commutateur.	8.5(1)	Bien que la connexion à l'ASASM à partir du commutateur en mode de contexte multiple se connecte à l'espace d'exécution du système, vous pouvez configurer l'authentification dans le contexte d'administration pour régir ces connexions.
Prise en charge de la politique de mot de passe administrateur lors de l'utilisation de la base de données locale	8.4(4.1), 9.1(2)	Lorsque vous configurez l'authentification pour l'accès à l'interface de ligne de commande ou à ASDM à l'aide de la base de données locale, vous pouvez configurer une politique de mot de passe qui oblige un utilisateur à changer de mot de passe après une durée spécifiée et qui exige également des normes de mot de passe tel qu'une longueur minimum et le nombre minimum de modifications de caractères. Nous avons introduit l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > Password Policy (Politique de mot de passe).

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de l'authentification par clé publique SSH	8.4(4.1), 9.1(2)	Vous pouvez activer l'authentification par clé publique pour les connexions SSH à l'ASA par utilisateur. Vous pouvez spécifier une clé formatée de fichier de clé publique (PKF) ou une clé Base64. La clé PKF peut comporter jusqu'à 4 096 bits. Utilisez le format PKF pour les clés qui sont trop grandes pour la prise en charge ASA du format Base64 (jusqu'à 2 048 bits). Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs) > Edit User Account (Modifier le compte d'utilisateur) > Public Key Authentication (Authentification par clé publique) Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs) > Edit User Account (Modifier le compte d'utilisateur) > Public Key Using PKF (Clé publique utilisant PKF). *Le format de clé PKF est uniquement pris en charge dans la version 9.1(2) et les versions ultérieures.*
Prise en charge du groupe Diffie-Hellman 14 pour l'échange de clés SSH	8.4(4.1), 9.1(2)	La prise en charge du groupe Diffie-Hellman 14 pour l'échange de clés SSH a été ajoutée. Auparavant, seul le groupe 1 était pris en charge. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ASDM/HTTPS/Telnet/SSH.
Prise en charge d'un nombre maximum de sessions de gestion	8.4(4.1), 9.1(2)	Vous pouvez définir le nombre maximum de sessions ASDM, SSH et Telnet simultanées. Nous avons introduit l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > Management Session Quota (Quota de sessions de gestion).
Sécurité SSH améliorée; le nom d'utilisateur SSH par défaut n'est plus pris en charge.	8.4(2)	À partir de la version 8.4(2), vous ne pouvez plus vous connecter à l'ASA à l'aide de SSH avec le nom d'utilisateur pix ou asa et le mot de passe de connexion. Pour utiliser SSH, vous devez configurer l'authentification AAA à l'aide de la commande **aaa authentication ssh console LOCAL** (interface de ligne de commande) ou Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authentication (ASDM) (Authentification (ASDM)); puis définissez un utilisateur local en saisissant la commande **username** (interface de ligne de commande) ou en sélectionnant Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (ASDM) (Comptes d'utilisateurs (ASDM)). Si vous souhaitez utiliser un serveur AAA pour l'authentification au lieu de la base de données locale, nous vous conseillons de configurer également l'authentification locale comme méthode de sauvegarde.

Nom de la caractéristique	Versions de plateforme	Description
Accès de gestion	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ASDM/HTTPS/Telnet/SSH Configuration (Configuration ASDM/HTTPS/Telnet/SSH) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > Command Line (CLI) Ligne de commande (Interface de ligne de commande) > Banner Configuration (Configuration de la bannière) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > CLI Prompt Configuration (Configuration de l'invite de l'interface de ligne de commande) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ICMP Configuration (Configuration ICMP) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > FTP Client Configuration (Configuration du client FTP) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > Secure Copy (SCP) Server Configuration (Configuration du serveur de copie sécurisée) > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > File Access (Accès au fichier) > Mount-Points Configuration (Configuration des points de montage) > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authentication Configuration (Configuration de l'authentification) > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authorization Configuration (Configuration de l'autorisation) > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Accounting (Comptabilisation).

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.