Paramètres de Gestionnaire de châssis

Firepower 2100 exécute FXOS pour contrôler les opérations de base du dispositif. Vous pouvez utiliser l'interface graphique utilisateur du Gestionnaire de châssis ou de l'interface de ligne de commande de FXOS pour configurer ces fonctions. Ce document couvre le gestionnaire de châssis. Notez que toutes les politiques de sécurité et autres opérations sont configurées dans le système d'exploitation de l'ASA (à l'aide de l'interface de ligne de commande ou d'ASDM).

Aperçu

Sous l'onglet **Overview** (Vue d'ensemble), vous pouvez facilement surveiller l'état du châssis Firepower 2100. L'onglet **Overview** (Vue d'ensemble) fournit les éléments suivants :

- Device Information (Informations sur le dispositif) : la partie supérieure de l'onglet **Overview** (Vue d'ensemble) contient les informations suivantes sur Firepower 2100 :
  - Chassis name (Nom du châssis) : affiche le nom attribué au châssis. Par défaut, le nom est **firepower-***modèle*, par exemple, firepower-2140. Ce nom apparaît dans l'invite de l'interface de ligne de commande. Pour modifier le nom du châssis, utilisez la commande de l'Interface de ligne de commande FXOS **scope system / set name**.
  - IP address (adresse IP) : indique l'adresse IP de gestion attribuée au châssis.
  - Model (Modèle) : indique le modèle du châssis Firepower 2100.
  - Version (Version) : indique le numéro de version de l'ASA exécuté sur le châssis.
  - Operational State (État opérationnel) : indique l'état opérationnel du châssis.
  - Chassis uptime (Temps de fonctionnement du châssis) : indique le temps écoulé depuis le dernier redémarrage du système.

- Uptime Information Icon (Icône d'information sur le temps de fonctionnement) : passez au-dessus de l'icône pour afficher les temps de fonctionnement du châssis et du moteur de sécurité de l'ASA.

- Visual Status Display (Affichage de l'état visuel) : au-dessous de la section Device Information (Informations sur le dispositif), il y a une représentation visuelle du châssis qui indique les composants installés dans le châssis et fournit un état général de ces composants. Vous pouvez passer le curseur sur les ports affichés dans l'affichage visuel de l'état pour obtenir des renseignements supplémentaires comme interface name (nom de l'interface), speed (vitesse), type (type), admin state (état d'administration) et operational state (état opérationnel).
- Detailed Status Information (Informations détaillées sur l'état) : sous l'affichage visuel de l'état se trouve un tableau contenant des informations détaillées sur l'état du châssis. Les renseignements sur l'état sont divisés en ces sections : défaillances, interfaces, dispositifs et inventaire. Vous pouvez voir un résumé pour chacune de ces sections au-dessus du tableau et vous pouvez voir des détails supplémentaires pour chacune de ces sections en cliquant sur la zone récapitulative des renseignements que vous souhaitez afficher.

  Le système fournit les informations détaillées sur l'état du châssis :

  - **Faults** (Défaillances) : répertorie les défaillances qui ont été générées dans le système. Les défaillances sont triées par gravité : critique, majeure, mineure, avertissement et information. Pour chaque défaillance répertoriée, vous pouvez afficher la gravité, une description de la défaillance, la cause, le nombre d'occurrences et l'heure de la défaillance la plus récente. Vous pouvez également vérifier si on a accusé réception de la défaillance ou non.

    Vous pouvez cliquer sur l'une des défaillances pour afficher des détails supplémentaires ou pour en accuser réception.

Remarque Une fois que la cause sous-jacente de la défaillance a été traitée, cette dernière sera automatiquement supprimée de la liste lors du prochain intervalle d'interrogation. Si un utilisateur travaille sur une résolution pour une défaillance en particulier, il peut en accuser réception pour faire savoir aux autres utilisateurs que la défaillance est actuellement en cours de traitement.

  - **Interfaces** (Interfaces) : répertorie les interfaces installées dans le système et indique le nom de l'interface, l'état opérationnel, l'état administratif, le nombre d'octets reçus et le nombre d'octets transmis.

    Vous pouvez cliquer sur n'importe quelle interface pour afficher une représentation graphique du nombre d'octets entrants et sortants de cette interface au cours des quinze dernières minutes.

  - **Devices** (Dispositifs) : indique l'ASA et fournit les détails suivants : nom du dispositif, état du dispositif, application, état opérationnel, état administratif, version de l'image et adresse IP de gestion.
  - **Inventory** (Inventaire) : répertorie les composants installés sur le châssis et fournit des détails pertinents pour ces composants, notamment : le nom du **component** (composant), le nombre de cœurs, l'emplacement d'installation, l'état opérationnel, la fonctionnalité, la capacité, l'alimentation, la protection thermique, le numéro de série, le numéro de modèle, le numéro de pièce et le fournisseur.

Interfaces

Vous pouvez gérer les interfaces physiques dans FXOS. Pour utiliser une interface, elle doit être physiquement activée dans FXOS et logiquement activée dans l'ASA.

Le châssis Firepower 2100 prend en charge les bâtis grand format activés par défaut. L'unité de transfert maximale est de 9184.

Remarque Si vous modifiez les interfaces dans FXOS après avoir activé le basculement (p. ex., en ajoutant ou en supprimant un module de réseau ou en modifiant la configuration EtherChannel), modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

Si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation de l'ASA.

Interfaces de configuration

Vous pouvez physiquement activer et désactiver les interfaces, ainsi que définir la vitesse d'interface et le mode duplex. Pour utiliser une interface, elle doit être physiquement activée dans FXOS et logiquement activée dans l'ASA.

Procédure

Étape 1 Cliquez sur l'onglet **Interfaces** (Interfaces).

Étape 2 Pour activer ou désactiver une interface, cliquez sur le curseur **Admin State** (État d'administration). Une coche indique qu'il est activé, tandis qu'un X l'affiche comme désactivé.

Remarque
L'interface de gestion Management 1/1 apparaît comme **MGMT** dans ce tableau.

Étape 3 Cliquez sur l'icône **Modifier** en forme de crayon de l'interface pour laquelle vous souhaitez modifier la vitesse ou le mode duplex.

Remarque
Vous pouvez uniquement activer ou désactiver l'interface Management 1/1; vous ne pouvez pas modifier ses propriétés.

Étape 4 Cochez la case **Enable** (activer) pour activer l'interface.

Étape 5 Dans la liste déroulante **Admin Speed** (Vitesse d'administration), choisissez la vitesse de l'interface.

Étape 6 Cliquez sur le bouton radio **Yes** (Oui) ou **No** (Non) pour **Auto Negotiation** (Négociation automatique).

Étape 7 Dans la liste déroulante **Admin Duplex** (Duplex d'administration), choisissez l'option de duplex pour l'interface.

Étape 8 Cliquez sur **OK**.

Ajouter un canal EtherChannel

Un canal EtherChannel (également appelé canal de port) peut inclure jusqu'à 8 interfaces membres de même type de support et de capacité, et doit être réglé à la même vitesse et au même duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité.

Remarque Les ports membres EtherChannel sont visibles sur l'ASA, mais vous pouvez uniquement configurer les canaux EtherChannel et les ports membres dans FXOS.

Si vous modifiez la configuration des canaux EtherChannel après avoir activé le basculement, modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

Remarque L'ASA ne prend pas en charge le débit LACP rapide; le protocole LACP utilise toujours le débit normal.

Avant de commencer

Firepower 2100 prend en charge les canaux EtherChannel en mode Active (Actif) ou On (Activé) du protocole LACP (Link Aggregation Control Protocol). Par défaut, le mode LACP est défini sur « Active »; vous pouvez changer le mode pour qu'il soit réglé sur « On » au niveau de l'interface de ligne de commande. Nous vous suggérons de régler les ports de connexion du commutateur sur le mode Active (Actif) pour une meilleure compatibilité.

Procédure

Étape 1 Cliquez sur l'onglet **Interfaces** (Interfaces).

Étape 2 Cliquez sur **Add Port Channel** (Ajouter un canal de port) au-dessus du tableau des interfaces.

Étape 3 Dans le champ **Port Channel ID** (Identifiant de canal de port), entrez un numéro identifiant le canal de port. Les valeurs valides sont comprises entre 1 et 47.

Étape 4 Cochez la case **Enable** (Activer) pour activer le canal de port.

Ignorer la liste déroulante **Type** (Type); le seul type disponible est **Data** (Données).

Étape 5 Dans la liste déroulante **Admin Speed** (Vitesse d'administration), choisissez la vitesse pour toutes les interfaces membres.

Si vous choisissez des interfaces qui ne sont pas capables de respecter la vitesse (et d'autres paramètres sélectionnés), la vitesse la plus rapide possible sera automatiquement appliquée.

Étape 6 Cliquez sur le bouton radio **Auto Negotiation** (Négotiation automatique) **Yes** (Oui) ou **No** (Non) pour toutes les interfaces membres.

Étape 7 Dans la liste déroulante **Admin Duplex** (Duplex d'administration), choisissez le duplex pour toutes les interfaces membres.

Étape 8 Dans la liste **Available Interface** (Interfaces disponibles), sélectionnez l'interface que vous souhaitez ajouter, puis cliquez sur **Add Interface** (Ajouter l'interface).

Vous pouvez ajouter jusqu'à 8 interfaces.

Astuces

Vous pouvez ajouter plusieurs interfaces en même temps. Pour sélectionner plusieurs interfaces, cliquez sur les interfaces souhaitées tout en maintenant la touche **Ctrl** enfoncée. Pour sélectionner une plage d'interfaces, sélectionnez la première interface de la plage, puis, tout en maintenant la touche **Shift** (Maj) enfoncée, cliquez pour sélectionner la dernière interface de la plage.

Remarque

Si vous affectez une interface à un canal EtherChannel, la configuration de l'ASA conserve les commandes de l'interface d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation de l'ASA.

Par exemple, après avoir affecté Ethernet1/4 au canal de port 7 dans FXOS, Ethernet1/4 apparaît toujours comme une interface disponible dans le système d'exploitation de l'ASA et toute configuration pour Ethernet1/4 est conservée. Si vous saisissez **show interface ethernet1/4**, l'ASA indique que l'interface n'est « pas associée au superviseur ». Utilisez la commande **no interface ethernet1/4** pour supprimer la configuration superflue.

Étape 9 Cliquez sur **OK**.

Surveillance des interfaces

Sous l'onglet **Interfaces**, vous pouvez afficher l'état des interfaces installées sur le châssis. La section inférieure contient un tableau des interfaces installées sur le châssis. La section supérieure affiche une représentation visuelle des interfaces installées sur le châssis. Vous pouvez passer le curseur sur n'importe quelle interface dans la section supérieure pour obtenir des informations supplémentaires sur cette dernière.

Les interfaces comportent un code de couleur pour indiquer leur état actuel :

- Vert : l'état opérationnel est Up (En fonction).
- Gris sombre : l'admin state (état d'administration) est Disabled (Désactivé).
- Rouge : l'état opérationnel est Down (Pas en fonction).
- Gris clair : le module SFP n'est pas installé.

Dispositifs logiques

La page **Logical Devices** (Dispositifs logiques) affiche les informations et l'état de l'ASA. Vous pouvez également désactiver ou réactiver l'ASA à des fins de dépannage en utilisant le curseur (une coche indique qu'il est activé, tandis qu'un X indique qu'il est désactivé).

L'en-tête de l'ASA indique le **Status** (État) :

- **ok** : la configuration du dispositif logique est terminée.
- **incomplete-configuration** (configuration-incomplète) : la configuration du dispositif logique est incomplète.

La zone du dispositif logique fournit également un **Status** (État) plus détaillé de l'ASA :

- **Online** (En ligne) : l'ASA est en cours d'exécution et fonctionne.
- **Offline** (Hors ligne) : l'ASA est arrêté et ne fonctionne plus.
- **Installing** (Installation en cours) : l'installation de l'ASA est en cours.
- **Not Installed** (Non installé) : l'ASA n'est pas installé.
- **Install Failed** (Échec de l'installation) : l'installation de l'ASA a échoué.
- **Starting** (Démarrage) : l'ASA démarre.
- **Start Failed** (Échec du démarrage) : l'ASA n'a pas pu démarrer.
- **Started** (Démarré) : l'ASA a démarré avec succès et attend le message pulsion de l'application.
- **Stopping** (Arrêt en cours) : l'ASA est en cours d'arrêt.
- **Stop Failed** (Échec de l'arrêt) : l'ASA n'a pas pu être déconnecté.
- **Not Responding** (Ne répond pas) : l'ASA ne répond pas.
- **Updating** (Mise à niveau en cours) : la mise à niveau du logiciel de l'ASA est en cours
- **Update Failed** (Échec de la mise à jour) : la mise à niveau du logiciel de l'ASA a échoué.
- **Update Succeeded** (Mise à jour réussie) : la mise à niveau du logiciel de l'ASA a réussi.

Paramètres de la plateforme

L'onglet **Platform Settings** (Paramètres de la plateforme) vous permet de définir les opérations de base pour FXOS, y compris l'heure et l'accès administratif.

NTP : définir l'heure

Vous pouvez régler l'horloge manuellement ou utiliser un serveur NTP (méthode recommandée). Vous pouvez configurer jusqu'à quatre serveurs NTP.

Avant de commencer

- NTP est configuré par défaut avec les serveurs NTP de Cisco suivants : 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
- Si vous utilisez un nom d'hôte pour le serveur NTP, vous devez configurer un serveur DNS. Consultez DNS : configurer des serveurs DNS, à la page 17.

Procédure

Étape 1 Cliquez sur l'onglet **Platform Settings** (Paramètres de la plateforme), puis sur **NTP** dans le menu de navigation de gauche.

L'onglet **Time Synchronization** (Synchronisation de l'heure) est sélectionné par défaut.

Étape 2 Pour utiliser un serveur NTP :

a) Cliquez sur le bouton radio **Use NTP Server** (Utiliser le serveur NTP).

b) (Facultatif) (ASA 9.10[1] ou versions ultérieures) Cochez la case **NTP Server Authentication: Enable** (Authentification du serveur NTP : activer) si vous devez vous authentifier auprès du serveur NTP.

Cliquez sur **Yes** (Oui) pour exiger un identifiant et une valeur de clé d'authentification.

Seul SHA1 est pris en charge pour l'authentification du serveur NTP.

c) Cliquez sur **Add** (Ajouter) pour identifier jusqu'à 4 serveurs NTP par adresse IP ou nom d'hôte.

Si vous utilisez un nom d'hôte pour le serveur NTP, configurez un serveur DNS plus tard dans cette procédure.

d) (ASA 9.10[1] et versions ultérieures) Saisissez l'identifiant de **Authentication Key** (Clé d'authentification) et la **Authentication Value** (Valeur d'authentification) du serveur NTP.

Obtenez l'identifiant et la valeur de la clé du serveur NTP. Par exemple, pour générer la clé SHA1 sur le serveur NTP version 4.2.8p8 ou ultérieure avec OpenSSL installé, saisissez la commande **ntp-keygen -M** , puis affichez l'ID de clé et la valeur dans le fichier ntp.keys. La clé est utilisée pour indiquer au client et au serveur quelle valeur utiliser lors du calcul du condensé du message.

e) Cliquez sur **Save** (Enregistrer) pour enregistrer la règle.

Étape 3 Pour régler l'heure manuellement :

a) Cliquez sur le bouton radio **Set Time Manually** (Définir l'heure manuellement).

b) Cliquez sur la liste déroulante **Date** (Date) pour afficher un calendrier, puis définissez la date à l'aide des contrôles disponibles dans le calendrier.

c) Utilisez les listes déroulantes correspondantes pour préciser les heures, les minutes et **AM/PM** (matin/soir).

Étape 4 Cliquez sur l'onglet **Current Time** (Heure actuelle) et dans la liste déroulante **Time Zone** (Fuseau horaire), choisissez le fuseau horaire approprié pour le châssis.

Étape 5 Cliquez sur **Save** (Enregistrer).

Remarque
Si vous modifiez l'horloge système de plus de 10 minutes, le système vous déconnectera et vous devrez vous reconnecter au Cisco Secure Firewall chassis manager.

SSH : configurer SSH

La procédure suivante décrit comment activer ou désactiver l'accès SSH au châssis, et comment activer le châssis en tant que client utilisant le protocole SSH. Le serveur et le client SSH sont activés par défaut.

Procédure

Étape 1 Choisissez **Platform Settings (Paramètres de plateforme)** > **SSH** > **SSH Server (Serveur SSH)**.

Étape 2 Pour permettre au serveur SSH d'autoriser l'accès SSH au châssis, activez le curseur **Enable SSH** (Activer le protocole SSH).

Étape 3 Pour l'**Encryption Algorithm** (Algorithme de chiffrement) du serveur, cochez les cases de chaque algorithme de chiffrement autorisé.

Étape 4 Pour le **Key Exchange Algorithm** (Algorithme d'échange de clés) du serveur, cochez les cases pour chaque échange de clés Diffie-Hellman (DH) autorisé.

L'échange de clés DH fournit un secret partagé qui ne peut être déterminé par aucune des parties à elles seules. L'échange de clé est combiné à une signature et à la clé de l'hôte pour authentifier l'hôte. Cette méthode d'échange de clés fournit une authentification explicite du serveur. Pour en savoir plus sur l'utilisation des méthodes d'échange de clés DH, consultez la RFC 4253.

Étape 5 Pour le **Mac Algorithm** (Algorithme Mac) du serveur, cochez les cases de chaque algorithme d'intégrité autorisé.

Étape 6 Pour la **Host Key** (Clé de l'hôte) du serveur, saisissez la taille de module pour les paires de clés RSA.

La valeur du module (en bits) est un multiple de 8 de 1024 à 2048. Plus la taille du module de clé que vous spécifiez est grande, plus il faut de temps pour générer une paire de clés RSA. Nous recommandons une valeur de 2048.

Étape 7 Pour la **Volume Rekey Limit** (Limite de renouvellement de volume) du serveur, définissez la quantité de trafic en Ko autorisé sur la connexion avant que FXOS ne déconnecte la session.

Étape 8 Pour la valeur **Time Rekey Limit** (Limite de renouvellement du temps) du serveur, définissez le nombre de minutes pendant lesquelles une session SSH peut être inactive avant que FXOS ne déconnecte la session.

Étape 9 Cliquez sur **Save** (Enregistrer).

Étape 10 Cliquez sur l'onglet **SSH Client** (Client SSH) pour personnaliser le client SSH du châssis FXOS.

Étape 11 Pour la **Strict Host Keycheck** (Vérification de la clé de l'hôte strict), choisissez **enable** (activer), **disable** (désactiver) ou **prompt** (inviter) pour contrôler la vérification de la clé d'hôte SSH.

- **enable** (activer) : la connexion est rejetée si la clé d'hôte ne figure pas déjà dans le fichier des hôtes connus de FXOS. Vous devez ajouter manuellement des hôtes au niveau de l'interface de ligne de commande de FXOS à l'aide de la commande **enter ssh-host** dans la portée system/services (systèmes/services).
- **prompt** (inviter) : vous êtes invité à accepter ou à refuser la clé d'hôte si elle n'est pas déjà stockée sur le châssis.
- **disable** (désactiver) : (valeur par défaut) le châssis accepte automatiquement la clé d'hôte si elle n'a pas été stockée auparavant.

Étape 12 Pour l'**Encryption Algorithm** (Algorithme de chiffrement) du client, cochez les cases de chaque algorithme de chiffrement autorisé.

Étape 13 Pour le **Key Exchange Algorithm** (Algorithme d'échange de clés) du client, cochez les cases pour chaque échange de clés Diffie-Hellman (DH) autorisé.

L'échange de clés DH fournit un secret partagé qui ne peut être déterminé par aucune des parties à elles seules. L'échange de clé est combiné à une signature et à la clé de l'hôte pour authentifier l'hôte. Cette méthode

d'échange de clés fournit une authentification explicite du serveur. Pour en savoir plus sur l'utilisation des méthodes d'échange de clés DH, consultez la RFC 4253.

Étape 14 Pour le **Mac Algorithm** (Algorithme Mac) du client, cochez les cases de chaque algorithme d'intégrité autorisé.

Étape 15 Pour la **Volume Rekey Limit** (Limite de renouvellement de volume) du client, définissez la quantité de trafic en Ko autorisé sur la connexion avant que FXOS ne déconnecte la session.

Étape 16 Pour la **Time Rekey Limit** (Limite de renouvellement du temps) du client, définissez le nombre de minutes pendant lesquelles une session SSH peut être inactive avant que FXOS ne déconnecte la session.

Étape 17 Cliquez sur **Save** (Enregistrer).

SNMP : configurer le SNMP

Utilisez la page **SNMP** pour configurer le protocole Simple Network Management Protocol (SNMP) sur le châssis.

À propos de SNMP

SNMP est un protocole de couche application qui fournit un format de message pour assurer la communication entre les agents et les gestionnaires SNMP. SNMP fournit un cadre normalisé et un langage commun utilisés pour la surveillance et la gestion des dispositifs dans un réseau.

Le cadre SNMP comprend trois parties :

- Un SNMP manager (Gestionnaire SNMP) : le système utilisé pour contrôler et surveiller les activités des dispositifs réseau à l'aide de SNMP.
- Un SNMP agent (Agent SNMP) : le composant logiciel dans le châssis qui conserve les données pour le châssis et qui transmet les données, au besoin, au gestionnaire SNMP. Le châssis comprend l'agent et un ensemble de MIB.
- Une base d'information gérée (MIB) : l'ensemble des objets gérés sur l'agent SNMP.

Le châssis prend en charge SNMPv1, SNMPv2c et SNMPv3. Les protocoles SNMPv1 et SNMPv2c utilisent tous deux une forme de sécurité basée sur la communauté.

Pour en savoir plus sur les MIB prises en charge, consultez le Cisco Firepower 2100 FXOS MIB Reference Guide (Guide de référence sur les MIB FXOS du châssis Cisco Firepower 2100).

Notifications SNMP

Une fonctionnalité clé de SNMP est la capacité de générer des notifications à partir d'un agent SNMP. Ces notifications ne nécessitent pas l'envoi de demandes par l'entremise du gestionnaire SNMP. Les notifications peuvent indiquer une authentification d'utilisateur incorrecte, des redémarrages, la fermeture d'une connexion, la perte de connexion à un routeur voisin ou d'autres événements importants.

Le châssis génère des notifications SNMP sous forme d'interruptions ou d'informations. Les interruptions sont moins fiables que les informations, car le gestionnaire SNMP n'envoie pas d'accusé de réception lorsqu'il reçoit une interruption et le châssis ne peut pas déterminer si l'interruption a été reçue. Un gestionnaire SNMP qui reçoit une demande d'information accuse réception du message auprès d'une unité de données de protocole (PDU) de réponse SNMP. Si le châssis ne reçoit pas la PDU, il peut renvoyer la demande d'information.

Niveaux de sécurité et privilèges SNMP

SNMPv1, SNMPv2c et SNMPv3 représentent chacun un modèle de sécurité différent. Le modèle de sécurité se combine avec le niveau de sécurité sélectionné pour déterminer le mécanisme de sécurité appliqué lors du traitement du message SNMP.

Le niveau de sécurité détermine les privilèges requis pour afficher le message associé à une interruption SNMP. Le niveau de privilège détermine si le message doit être protégé contre toute divulgation ou s'il doit être authentifié. Le niveau de sécurité pris en charge dépend du modèle de sécurité mis en œuvre. Les niveaux de sécurité SNMP prennent en charge un ou plusieurs des privilèges suivants :

- noAuthNoPriv : pas d'authentification ni de chiffrement
- authNoPriv : authentification, mais sans chiffrement
- authPriv : authentification et chiffrement

SNMPv3 prend en charge les modèles et les niveaux de sécurité. Un modèle de sécurité est une méthode d'authentification configurée pour un utilisateur et le rôle dans lequel l'utilisateur réside. Un niveau de sécurité est le niveau de sécurité autorisé dans un modèle de sécurité. Une combinaison d'un modèle de sécurité et d'un niveau de sécurité détermine quel mécanisme de sécurité est utilisé lors du traitement d'un paquet SNMP.

Combinaisons de modèles et de niveaux de sécurité SNMP prises en charge

Le tableau suivant répertorie la signification des combinaisons de modèles et de niveaux de sécurité.

Tableau 1 : Modèles et niveaux de sécurité SNMP

Modèle	Niveau	Authentification	Chiffrement	Que se passe-t-il?
v1	noAuthNoPriv	Chaîne de communauté	Aucun	Utilise une correspondance de chaîne de communauté pour l'authentification.
v2c	noAuthNoPriv	Chaîne de communauté	Aucun	Utilise une correspondance de chaîne de communauté pour l'authentification.
v3	noAuthNoPriv	Nom de l'utilisateur	Aucun	Utilise une correspondance de nom d'utilisateur pour l'authentification.
v3	authNoPriv	HMAC-SHA	Non	Fournit une authentification basée sur l'algorithme de hachage sécurisé (SHA) HMAC.
v3	authPriv	HMAC-SHA	DES	Fournit une authentification basée sur l'algorithme HMAC-SHA. Fournit un standard de chiffrement des données (DES) à 56 bits en plus de l'authentification basée sur le standard de chaîne de bloc de chiffres (CBC) DES (DES-56).

Fonctions de sécurité SNMPv3

SNMPv3 offre un accès sécurisé aux dispositifs par l'entremise d'une combinaison d'authentification et de chiffrement des paquets sur le réseau. SNMPv3 autorise les opérations de gestion uniquement par les utilisateurs configurés et chiffre les messages SNMP. Le modèle de sécurité basé sur l'utilisateur (USM) SNMPv3 fait référence à la sécurité au niveau des messages SNMP et offre les services suivants :

- Message integrity (Intégrité des messages) : garantit que les messages n'ont pas été modifiés ou détruits de manière non autorisée et que les séquences de données n'ont pas été modifiées de manière plus importante par rapport à ce qui peut se produire de manière non malveillante.
- Message origin authentication (Authentification de l'origine du message) : garantit que l'identité revendiquée de l'utilisateur au nom duquel les données reçues ont été produites est confirmée.
- Message confidentiality and encryption (Confidentialité et chiffrement des messages) : veille à ce que les informations ne soient pas mises à la disposition ou divulguées à des personnes, à des entités ou des processus non autorisés.

Prise en charge de SNMP

Le châssis offre les services de prise en charge suivants pour SNMP :

Prise en charge des MIB

Le châssis prend en charge l'accès en lecture seule aux MIB. Pour en savoir plus sur les MIB prises en charge, consultez le Cisco Firepower 2100 FXOS MIB Reference Guide (Guide de référence sur les MIB FXOS du châssis Cisco Firepower 2100).

Protocole d'authentification pour les utilisateurs SNMPv3

Le châssis prend en charge le protocole d'authentification HMAC-SHA-96 (SHA) pour les utilisateurs SNMPv3.

Protocole de confidentialité AES pour les utilisateurs SNMPv3

Outre l'authentification basée sur le protocole SHA, le châssis assure également la confidentialité des données à l'aide du standard de chiffrement avancé AES-128 bits. Le châssis utilise le mot de passe de confidentialité pour générer une clé AES de 128 bits. Le mot de passe de confidentialité d'AES peut comporter au moins huit caractères. Si les phrase secrètes sont spécifiées en texte clair, vous pouvez spécifier un maximum de 80 caractères.

Configurer SNMP

Activez SNMP, ajoutez des déroutements et des utilisateurs SNMPv3.

Procédure

Étape 1 Choisissez **Platform Settings (Configurations de plateforme)** > **SNMP**.

Étape 2 Dans la zone **SNMP**, remplissez les champs comme suit :

Nom	Description
Case à cocher **Admin State** (État d'administration)	Si SNMP est activé ou désactivé. Activez ce service uniquement si votre système comprend une intégration avec un serveur SNMP.
Champ **Port** (Port)	Port sur lequel le châssis Firepower communique avec l'hôte SNMP. Vous ne pouvez pas modifier le port par défaut.

Nom	Description
Champ **Community/Username** (Communauté / nom d'utilisateur)	Le nom de communauté SNMP v1 ou v2 ou le nom d'utilisateur SNMP v3 par défaut que le châssis Firepower inclut dans tous les messages de déroutement qu'il envoie à l'hôte SNMP. Saisissez une chaîne alphanumérique comprise entre 1 et 32 caractères. N'utilisez pas @ (at), \ (barre oblique inverse), « (guillemets), ? (point d'interrogation) ou un espace vide. La valeur par défaut est **`public`**. Notez que si le champ **Community/Username** (Communauté / nom d'utilisateur) est déjà défini, le texte à droite du champ vide indique **Set: Yes** (Définir : oui). Si le champ **Community/Username** (Communauté / nom d'utilisateur) ne contient pas encore de valeur, le texte à droite du champ vide indique **Set: No** (Définir : non).
Champ **System Administrator Name** (Nom de l'administrateur du système)	La personne-ressource responsable de l'implémentation de SNMP. Saisissez une chaîne de 255 caractères maximum, comme une adresse de courriel ou un nom et un nom distinctif.
Champ **Location** (Emplacement)	Emplacement de l'hôte sur lequel l'agent SNMP (serveur) est exécuté. Saisissez une chaîne alphanumérique de 510 caractères maximum.

Étape 3 Dans la zone **SNMP Traps** (Déroutements SNMP), cliquez sur **Add** (Ajouter).

Étape 4 Dans la boîte de dialogue **Add SNMP Trap** (Ajouter un déroutement SNMP), remplissez les champs suivants :

Nom	Description
Champ **Host Name** (Nom d'hôte)	Le nom d'hôte ou l'adresse IP de l'hôte SNMP auquel le châssis Firepower doit envoyer le déroutement.
Champ **Community/Username** (Communauté / nom d'utilisateur)	Le nom de communauté SNMP v1 ou v2 ou le nom d'utilisateur SNMPv3 que le châssis Firepower inclut lorsqu'il envoie le déroutement à l'hôte SNMP. Il doit s'agir de la communauté ou du nom d'utilisateur configuré pour le service SNMP. Saisissez une chaîne alphanumérique comprise entre 1 et 32 caractères. N'utilisez pas @ (at), \ (barre oblique inverse), « (guillemets), ? (point d'interrogation) ou un espace vide.
Champ **Port** (Port)	Port sur lequel le châssis Firepower communique avec l'hôte SNMP pour le déroutement. Saisissez un entier entre 1 et 65 535.
Champ **Version** (Version)	La version et le modèle du SNMP utilisés pour le déroutement. Voici les options offertes : • **V1** • **V2** • **V3**

Nom	Description
Champ**Type** (Type)	Si vous sélectionnez **V2** ou **V3** pour la version, le type de déroutement à envoyer. Voici les options offertes : • **Traps** (Déroutements) • **Informs** (Informations)
Champ **v3 Privilege** (Privilège v3)	Si vous sélectionnez **V3** pour la version, le privilège associé au déroutement. Voici les options offertes : • **Auth** : Authentification mais pas de chiffrement • **Noauth** : Pas d'authentification ni de chiffrement • **Priv** : Authentification et chiffrement

Étape 5 Cliquez sur **OK** pour fermer la boîte de dialogue **Add SNMP Trap** (Ajouter un déroutement SNMP).

Étape 6 Dans la zone **SNMP Users** (Utilisateurs SNMP), cliquez sur **Add** (Ajouter).

Étape 7 Dans la boîte de dialogue **Add SNMP User** (Ajouter un utilisateur SNMP), remplissez les champs suivants :

Nom	Description
Champ **Name** (Nom)	Le nom d'utilisateur affecté à l'utilisateur SNMP. Saisissez jusqu'à 32 lettres ou chiffres. Le nom doit commencer par une lettre et vous pouvez également spécifier un _ (trait de soulignement), . (point), @ (at) et - (trait d'union).
Champ **Auth Type** (Type d'authentification)	Le type d'autorisation : **SHA**.
Case à cocher **Use AES-128** (Utiliser AES-128)	Si cette option est cochée, cet utilisateur utilise le chiffrement AES-128.
Champ **Password** (Mot de passe)	Le mot de passe de cet utilisateur.
Champ **Confirm Password** (Confirmer le mot de passe)	Le mot de passe est répété pour confirmation.
Champ **Privacy Password** (Mot de passe de confidentialité)	Le mot de passe de confidentialité de cet utilisateur.
Champ **Confirm Privacy Password** (Confirmer le mot de passe de confidentialité)	Le mot de passe de confidentialité est à nouveau utilisé à des fins de confirmation.

Étape 8 Cliquez sur **OK** pour fermer la boîte de dialogue **Add SNMP User** (Ajouter un déroutement SNMP).

Étape 9 Cliquez sur **Save** (Enregistrer).

HTTPS : modifier le port

Le service HTTPS est activé sur le port 443 par défaut. Vous ne pouvez pas désactiver le protocole HTTPS, mais vous pouvez modifier le port à utiliser pour les connexions HTTPS.

Avant de commencer

Ne modifiez pas le port HTTPS à une autre valeur que 443 si vous activez l'accès HTTPS sur les interfaces de données d'ASA; seul le port par défaut est pris en charge.

Procédure

Étape 1 Choisissez **Platform Settings (Configurations de plateforme)** > **HTTPS**.

Étape 2 Saisissez le port à utiliser pour les connexions HTTPS dans le champ **Port**. Indiquez un entier entre 1 et 65 535. Ce service est activé sur le port 443 par défaut.

Étape 3 Cliquez sur **Save** (Enregistrer).

Le châssis Firepower est configuré avec le port HTTPS indiqué.

Après la modification du port HTTPS, toutes les sessions HTTPS actuelles seront fermées. Les utilisateurs devront se reconnecter au Cisco Secure Firewall chassis manager en utilisant le nouveau port comme suit :

`https://<adresse_ip_de_gestion_du_châssis>:<port_de_gestion_du_châssis>`

où <*adresse_ip_de_gestion_du_châssis*> représente l'adresse IP ou le nom d'hôte du châssis Firepower que vous avez saisi lors de la configuration initiale et <*port_de_gestion_du_châssis*> est le port HTTPS que vous venez de configurer.

DHCP : configurer le serveur DHCP pour les clients de gestion

Vous pouvez activer un serveur DHCP pour les clients associés à l'interface de gestion Management 1/1. Par défaut, le serveur est activé avec la plage d'adresses suivante : 192.168.45.10 à 192.168.45.12. Si vous souhaitez modifier l'adresse IP de gestion, vous devez désactiver DHCP. Vous pouvez ensuite réactiver DHCP pour le nouveau réseau.

Procédure

Étape 1 Choisissez **Platform Settings (Configurations de plateforme)** > **DHCP**.

Étape 2 Cochez la case **Enable DHCP service** (Activer le service DHCP).

Étape 3 Entrez les adresses **Start IP** (IP de début) et **End IP** (IP de fin).

Étape 4 Cliquez sur **Save** (Enregistrer).

Syslog : configuration de la messagerie relative à la journalisation du système

Les journaux sont utiles pour les dépannages de routine et pour le traitement des incidents. Vous pouvez envoyer des messages de journalisation du système à la console Firepower 2100, à une session SSH ou à un fichier local.

Ces messages de journalisation du système s'appliquent uniquement au châssis FXOS. Pour les messages de journalisation du système d'ASA, vous devez configurer la journalisation dans la configuration de l'ASA.

Remarque Les destinations distantes ne sont pas prises en charge.

Procédure

Étape 1 Choisissez **Platform Settings (Configurations de plateforme)** > **Syslog (Journalisation du système)**.

Étape 2 Configuration de destinations locales :

a) cliquez sur l'onglet **Local Destinations** (Destinations locales).

b) Remplissez les champs comme suit :

Nom	Description
Console	
Admin State (État d'administration)	Cochez la case **Enable** (Activer) pour afficher les messages de journalisation du système sur la console.
Level (Niveau)	Cliquez sur le niveau de message le plus bas que vous souhaitez afficher sur la console. L'affichage du châssis Firepower se fera à partir de ce niveau. • **Emergencies** (Urgences) • **Alerts** (Alertes) • **Critical** (Critique)
Plateforme	
Admin State (État d'administration)	Les messages de journalisation du système de la plateforme sont toujours activés.

Nom	Description
Level (Niveau)	Choisissez le niveau de message le plus bas que vous souhaitez afficher. L'affichage du châssis Firepower se fera à partir de ce niveau. La valeur par défaut est **Informational** (Information). • **Emergencies** (Urgences) • **Alerts** (Alertes) • **Critical** (Critique) • **Errors** (Erreurs) • **Warnings** (Avertissements) • **Notifications** (Notifications) • **Information** (Informations) • **Debugging** (Débogage)
Fichier	
Admin State (État d'administration)	Cochez la case **Enable** (Activer) pour enregistrer les messages de journalisation du système dans un fichier.
Level (Niveau)	Choisissez le niveau de message le plus bas que vous souhaitez enregistrer. Le système enregistre ce niveau et les suivants. • **Emergencies** (Urgences) • **Alerts** (Alertes) • **Critical** (Critique) • **Errors** (Erreurs) • **Warnings** (Avertissements) • **Notifications** (Notifications) • **Information** (Informations) • **Debugging** (Débogage)
Nom	Définissez le nom du fichier, jusqu'à 16 caractères.
Taille	Précisez la taille de fichier maximale, en octets, avant que le système commence à écraser les messages les plus anciens avec les plus récents. La plage se situe entre 4096 et 4 194 304 octets.

c) Cliquez sur **Save** (Enregistrer).

Étape 3 Configurez les sources locales :

a) Cliquez sur l'onglet **Local Sources** (Sources locales).

b) Remplissez les champs comme suit :

Nom	Description
Faults Admin State (État d'administration des défaillances)	Indique si la journalisation des défaillances du système est activée ou non. Si la case **Enable** (Activer) est cochée, le châssis Firepower consigne toutes les défaillances du système.
Audits Admin State (État d'administration des audits)	Indique si la journalisation des audits est activée ou non. Si la case **Enable** (Activer) est cochée, le châssis Firepower consigne tous les événements de journalisation d'audits.
Events Admin State (État d'administration des événements)	Indique si la journalisation des événements du système est activée ou non. Si la case **Enable** (Activer) est cochée, le châssis Firepower consigne tous les événements du système.

c) Cliquez sur **Save** (Enregistrer).

DNS : configurer des serveurs DNS

Vous devez préciser un serveur DNS si le système nécessite la résolution des noms d'hôte en adresses IP. Vous pouvez configurer jusqu'à quatre serveurs DNS. Lorsque vous configurez plusieurs serveurs DNS, le système cherche les serveurs dans n'importe quel ordre aléatoire.

Avant de commencer

- Le DNS est configuré par défaut avec les serveurs OpenDNS suivants : 208.67.222.222, 208.67.220.220.

Procédure

Étape 1 Choisissez **Platform Settings (Configurations de plateforme)** > **DNS**.

Étape 2 Cochez la case **Enable DNS Server** (Activer le serveur DNS).

Étape 3 Pour chaque serveur DNS que vous souhaitez ajouter, jusqu'à un maximum de quatre, saisissez l'adresse IP du serveur DNS dans le champ **DNS Server** (Serveur DNS) et cliquez sur **Add** (Ajouter).

Étape 4 Cliquez sur **Save** (Enregistrer).

Étape 5 Cliquez sur l'onglet **Domain Name Configuration** (Configuration du nom de domaine), saisissez le **Domain name** (Nom de domaine) que vous souhaitez que le châssis ajoute en tant que suffixe aux noms sans qualification, puis cliquez sur **Add** (Ajouter).

Par exemple, si vous définissez le nom de domaine « example.com » et indiquez un serveur de journalisation du système sous le nom non qualifié de « jupiter », le châssis donnera le nom « jupiter.example.com ».

FIPS et Common Criteria : activer les modes FIPS et Common Criteria

Suivez ces étapes pour activer le mode FIPS ou Common Criteria (CC) sur votre châssis Firepower 2100.

Vous devez également activer le mode FIPS séparément sur l'ASA à l'aide de la commande **fips enable**. Sur l'ASA, il n'y a pas de paramètre distinct pour le mode Common Criteria. Toute restriction supplémentaire pour la conformité aux normes CC ou UCAPL doit être configurée conformément aux documents de la politique de sécurité Cisco.

Nous vous recommandons de définir d'abord le mode FIPS sur l'ASA, d'attendre que le dispositif se recharge, puis de définir le mode FIPS dans FXOS.

Procédure

Étape 1 Choisissez **Platform Settings (Paramètres de plateforme)** > **FIPS and Common Criteria (FIPS et Common Criteria)**.

Étape 2 Activez **FIPS** en cochant la case **Enable** (Activer).

Étape 3 Activez **Common Criteria** en cochant la case **Enable** (Activer).

Lorsque vous activez Common Criteria, la case à cocher **FIPS Enable** (Activation de FIPS) est activée par défaut.

Étape 4 Cliquez sur **Save** (Enregistrer).

Étape 5 Suivez les invites pour redémarrer le système.

Liste d'accès : configurer l'accès de gestion

Par défaut, le châssis Firepower 2100 permet l'accès HTTPS au gestionnaire de châssis et l'accès SSH sur le réseau Management 1/1 192.168.45.0/24. Si vous souhaitez autoriser l'accès à partir d'autres réseaux ou autoriser SNMP, vous devez ajouter ou modifier les listes d'accès.

Pour chaque bloc d'adresses IP (v4 ou v6), vous pouvez configurer jusqu'à 25 sous-réseaux différents pour chaque service.

Procédure

Étape 1 Choisissez **Platform Settings (Paramètres de plateforme)** > **Access List (Liste d'accès)**.

Étape 2 Dans la zone **IPv4 Access List** (Liste d'accès IPv4) :

a) Cliquez sur **Add** (ajouter).

b) Renseignez ce qui suit :

- **IP Address** (Adresse IP) : définit l'adresse IP. Saisissez **0.0.0.0** pour autoriser tous les réseaux.
- **Prefix Length** (Longueur du préfixe) : définit le masque de sous-réseau. Saisissez **0** pour autoriser tous les réseaux.
- **Protocol** (Protocole) : choisissez **HTTPS**, **SNMP**ou **SSH**.

c) Cliquez sur **OK**.

d) Répétez ces étapes pour ajouter des services supplémentaires pour chaque service.

Étape 3 Dans la zone **IPv6 Access List** (Liste d'accès IPv6) :

a) Cliquez sur **Add** (ajouter).

b) Renseignez ce qui suit :

- **IP Address** (Adresse IP) : définit l'adresse IP. Entrez :: pour autoriser tous les réseaux.
- **Prefix Length** (Longueur du préfixe) : définit la longueur du préfixe. Saisissez **0** pour autoriser tous les réseaux.
- **Protocol** (Protocole) : choisissez **HTTPS**, **SNMP**ou **SSH**.

c) Cliquez sur **OK**.

d) Répétez ces étapes pour ajouter des services supplémentaires pour chaque service.

Étape 4 Cliquez sur **Save** (Enregistrer).

Mises à jour du système

Cette tâche s'applique à un ASA autonome. Si vous souhaitez mettre à niveau une paire de basculement, consultez le Cisco ASA Upgrade Guide (Guide de mise à niveau d'ASA). Le processus de mise à niveau prend généralement entre 20 et 30 minutes.

Les images ASA, ASDM et FXOS sont regroupées en un seul ensemble. Les mises à jour de paquets sont gérées par FXOS; vous ne pouvez pas mettre à niveau l'ASA dans le système d'exploitation de l'ASA. Vous ne pouvez pas mettre à niveau l'ASA et FXOS séparément; ils sont toujours regroupés.

L'exception est pour ASDM, qui peut être mis à niveau à partir du système d'exploitation de l'ASA, de sorte que vous n'avez pas besoin d'utiliser uniquement l'image ASDM fournie. Les images ASDM que vous téléchargez manuellement ne s'affichent pas dans la liste d'images FXOS; vous devez les gérer à partir de l'ASA.

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

Avant de commencer

Assurez-vous que l'image que vous souhaitez télécharger est disponible sur votre ordinateur local.

Procédure

Étape 1 Sélectionnez **System (Systèmes)** > **Updates (Mises à jour)**.

La page des **Available Updates** (Mises à jour disponibles) affiche une liste des applications disponibles sur le châssis.

Étape 2 Cliquez sur **Upload Image** (Charger une image).

Étape 3 Cliquez sur **Browse** (Naviguer) pour accéder à l'image à charger et la sélectionner.

Étape 4 Cliquez sur **Upload** (charger).

L'image sélectionnée est chargée sur le châssis. L'intégrité de l'image est automatiquement vérifiée lorsqu'une nouvelle image est ajoutée au châssis. Si vous souhaitez la vérifier manuellement, cliquez sur **Verify** (Vérifier) (icône de coche).

Étape 5 Sélectionnez le paquet de l'ASA que vous souhaitez mettre à niveau, et cliquez sur **Upgrade** (Mettre à niveau).

Étape 6 Cliquez sur **Yes** (Oui) pour confirmer que vous souhaitez poursuivre l'installation, ou cliquez sur **No** (Non) pour annuler l'installation.

Vous serez déconnecté du gestionnaire de châssis pendant la mise à niveau.

Gestion des utilisateurs

Les comptes d'utilisateur sont utilisés pour accéder au châssis Firepower 2100. Ces comptes fonctionnent pour gestionnaire de châssis et pour l'accès SSH. L'ASA a des comptes d'utilisateurs et une authentification distincts.

À propos des comptes d'utilisateurs

Compte d'administration

Le compte d'administration est un compte d'utilisateur par défaut et ne peut pas être modifié ou supprimé. Ce compte est l'administrateur du système ou le compte superutilisateur, et dispose de tous les privilèges. Le mot de passe par défaut est **Admin123**.

Le compte d'administration est toujours actif et n'expire pas. Vous ne pouvez pas rendre le compte d'administration inactif dans les configurations.

Comptes d'utilisateurs authentifiés localement

Vous pouvez configurer jusqu'à 48 comptes d'utilisateurs locaux. Chaque compte d'utilisateur doit avoir un nom d'utilisateur et un mot de passe uniques.

Un compte d'utilisateur authentifié localement peut être activé ou désactivé par toute personne disposant de privilèges d'administrateur.

Lignes directrices des comptes d'utilisateurs

Noms d'utilisateur

Le nom d'utilisateur est utilisé comme identifiant de connexion pour le Cisco Secure Firewall chassis manager et l'Interface de ligne de commande FXOS. Lorsque vous attribuez des identifiants de connexion, tenez compte des directives et des restrictions suivantes :

- L'identifiant de connexion peut contenir entre 1 et 32 caractères, y compris les éléments suivants :

- Deux caractères alphabétiques
- N’importe quel chiffre
- _ (trait de soulignement)
- - (trait d’union)
- . (point)

- L’identifiant de connexion doit être unique.
- L’identifiant de connexion doit commencer par un caractère alphabétique. Il ne peut pas commencer par un chiffre ou un caractère spécial, comme un trait de soulignement.
- L’identifiant de connexion est sensible à la casse.
- Vous ne pouvez pas créer un identifiant de connexion composé uniquement de chiffres.
- Après avoir créé un compte d’utilisateur, vous ne pouvez pas modifier l’identifiant de connexion. Vous devez supprimer le compte d’utilisateur et en créer un nouveau.

Mots de passe

Un mot de passe est requis pour chaque compte d’utilisateur authentifié localement. Un utilisateur avec des privilèges d’administrateur peut configurer le système pour effectuer une vérification de la robustesse des mots de passe des utilisateurs. Si la vérification de la robustesse du mot de passe est activée, chaque utilisateur doit avoir un mot de passe fort.

Nous vous recommandons d’utiliser des mots de passe robustes pour chaque utilisateur. Si vous activez la vérification de la robustesse du mot de passe pour les utilisateurs authentifiés localement, FXOS rejette tout mot de passe qui ne répond pas aux exigences suivantes :

- Doit contenir un minimum de 8 caractères et un maximum de 127 caractères.

Remarque Vous pouvez éventuellement configurer une longueur de mot de passe minimale de 15 caractères dans le système, afin de vous conformer aux exigences Common Criteria.

- Doit contenir au moins un caractère alphabétique majuscule.
- Doit contenir au moins un caractère alphabétique minuscule.
- Doit inclure au moins un caractère non alphanumérique (spécial).
- Ne doit pas contenir un caractère répété plus de trois fois consécutives, comme aaabbb.
- Ne doit pas contenir trois chiffres ou lettres consécutifs dans n‘importe quel ordre, comme motdepasseABC ou motdepasse321.
- Ne doit pas être identique au nom d’utilisateur ou au nom d’utilisateur à l’envers.
- Doit passer une vérification effectuée à l’aide d’un dictionnaire de mots de passe. Par exemple, le mot de passe ne doit pas être basé sur un mot du dictionnaire standard.

- Ne doit pas contenir les symboles suivants : $ (signe de dollar), ? (point d'interrogation) et = (signe d'égalité).
- Ne doit pas être vide.

Ajouter un utilisateur

Ajoutez des utilisateurs locaux pour l'accès gestionnaire de châssis et Interface de ligne de commande FXOS.

Procédure

Étape 1 Choisissez **System (Système)** > **User Management (Gestion des utilisateurs)**.

Étape 2 Cliquez sur l'onglet **Local Users** (Utilisateurs locaux).

Étape 3 Cliquez sur **Add User** (Ajouter un utilisateur) pour ouvrir la boîte de dialogue **Add User** (Ajouter un utilisateur).

Étape 4 Remplir les champs suivants avec les renseignements requis sur l'utilisateur :

- **User Name** (Nom d'utilisateur) : définit le nom d'utilisateur. Ce nom doit être unique et respecter les directives et les restrictions relatives aux noms de compte d'utilisateur (voir Lignes directrices des comptes d'utilisateurs, à la page 20). Après avoir enregistré l'utilisateur, l'identifiant de connexion ne peut pas être modifié. Vous devez supprimer le compte d'utilisateur et en créer un nouveau.
- **First Name** (Prénom) : définit le prénom de l'utilisateur. Ce champ peut contenir jusqu'à 32 caractères.
- **Last Name** (Nom de famille) : le nom de famille de l'utilisateur. Ce champ peut contenir jusqu'à 32 caractères.
- **Email** (Adresse courriel) : définit l'adresse courriel de l'utilisateur.
- **Phone Number** (Numéro de téléphone) : définit le numéro de téléphone de l'utilisateur.
- **Password** (Mot de passe) et **Confirm Password (Confirmer le mot de passe)** : définissent le mot de passe associé à ce compte. Si vous activez la vérification de la robustesse du mot de passe, ce dernier doit être robuste, et FXOS rejettera tout mot de passe qui ne répond pas aux exigences de vérification de la robustesse (voir Configurer les paramètres utilisateur, à la page 23 et Lignes directrices des comptes d'utilisateurs, à la page 20).
- **Account Status** (État du compte) : définit l'état sur **Active** (Actif) ou **Inactive** (Inactif).
- **User Role** (Rôle d'utilisateur) : définit le rôle qui représente les privilèges que vous souhaitez attribuer au compte d'utilisateur. Tous les utilisateurs se voient attribuer le rôle **Read-Only** (En lecture seule) par défaut. Ce rôle ne peut pas être désélectionné. Pour attribuer le rôle d'administrateur, cliquez sur **Admin** (Administrateur) dans la fenêtre pour qu'il soit mis en surbrillance. Le rôle d'administrateur permet un accès en lecture et en écriture à la configuration. Les modifications des rôles d'utilisateur et des privilèges ne prennent effet que lors de la prochaine connexion de l'utilisateur. Si un utilisateur est connecté lorsque vous attribuez un nouveau rôle ou supprimez un rôle existant pour un compte d'utilisateur, la session active continue avec les rôles et privilèges précédents.
- **Account Expires** (Le compte expirera) : définit que ce compte expirera. Le compte ne peut pas être utilisé après la date indiquée dans le champ **Expiry Date** (Date d'expiration). Après avoir configuré un compte d'utilisateur avec une date d'expiration, vous ne pouvez pas reconfigurer le compte pour qu'il

n’expire pas. Vous pouvez toutefois configurer le compte avec la dernière date d’expiration disponible. Par défaut, les comptes d’utilisateur n’expirent pas.

- **Expiry Date** (Date d’expiration) : la date à laquelle le compte expire. La date doit être au format aaaa-mm-jj. Cliquez sur l’icône du calendrier à la fin de ce champ pour afficher un calendrier que vous pouvez utiliser pour sélectionner la date d’expiration.

Étape 5 Cliquez sur **Add** (ajouter).

Étape 6 Pour désactiver un utilisateur :

a) Pour l’utilisateur que vous souhaitez désactiver, cliquez sur le l’icône **Modifier** ( ).

Le compte d’utilisateur administrateur est toujours actif et vous ne pouvez pas le désactiver.

b) Dans la zone **Account Status** (État du compte), cliquez sur le bouton radio **Inactive** (inactif).

c) Cliquez sur **Save** (Enregistrer).

Configurer les paramètres utilisateur

Vous pouvez configurer les paramètres globaux pour tous les utilisateurs.

Procédure

Étape 1 Choisissez **System (Système)** > **User Management (Gestion des utilisateurs)**.

Étape 2 Cliquez sur l'onglet **Settings** (Paramètres).

Étape 3 Remplissez les champs suivants.

- **Default Authentication** (Authentification par défaut) : méthode par défaut avec laquelle un utilisateur est authentifié lors de la connexion à distance. Voici les options offertes :
  - **Local** (Local) : le compte d’utilisateur doit être défini localement sur le châssis.
  - **None** (Aucun) : si le compte d’utilisateur est local au châssis, aucun mot de passe n’est requis lorsque l’utilisateur se connecte à distance.
- **Password Strength Check** (Vérification de la robustesse du mot de passe) : si la case est cochée, tous les mots de passe des utilisateurs locaux doivent être conformes aux directives pour les mots de passe robustes (voir Lignes directrices des comptes d'utilisateurs, à la page 20). La vérification de la robustesse du mot de passe est activée par défaut.
- **History Count** (Nombre de l’historique) : le nombre de mots de passe uniques qu’un utilisateur doit créer avant de pouvoir réutiliser un mot de passe précédemment utilisé. Le nombre de l’historique est en ordre chronologique inverse, avec le mot de passe le plus récent en premier pour s’assurer que seul le mot de passe le plus ancien peut être réutilisé lorsque le seuil du nombre de l’historique est atteint. Cette valeur peut être comprise entre 0 et 15. Vous pouvez définir le champ **History Count** (Nombre de l’historique) à 0 pour désactiver le nombre de l’historique et permettre aux utilisateurs de réutiliser les mots de passe précédemment utilisés.

- **Change Interval** (Intervalle de modification) : le nombre d'heures auxquelles le nombre de modifications de mot de passe spécifié dans le champ **Change Count** (Nombre de modifications) est appliqué. Cette valeur peut aller de 1 à 745 heures. Par exemple, si la valeur de ce champ est définie à 48 et que la valeur du champ **Change Count** (Nombre de modifications) est définie à 2, un utilisateur authentifié localement ne peut apporter plus de 2 changements de mot de passe dans une période de 48 heures. Cochez la case à cocher pour activer cette fonction.
- **Change Count** (Nombre de modifications) : le nombre maximal de fois qu'un utilisateur authentifié localement peut modifier son mot de passe pendant l'intervalle de modification. Cette valeur peut être comprise entre 0 et 10.
- **No Change Interval** (Intervalle de non-modification) : le nombre minimal d'heures qu'un utilisateur authentifié localement doit attendre avant de modifier un nouveau mot de passe. Cette valeur peut aller de 1 à 745 heures. Cochez la case à cocher pour activer cette fonction.
- **Passphrase Expiration Days** (Délai d'expiration en jours de la phrase secrète) : définissez le délai d'expiration à une valeur entre 1 et 9999 jours. Par défaut, l'expiration est désactivée.
- **Passphrase Expiration Warning Period** (Période d'avertissement de l'expiration de la phrase secrète) : définissez le nombre de jours avant l'expiration pour avertir l'utilisateur de l'expiration de son mot de passe à chaque connexion, entre 0 et 9999. La valeur par défaut est de 14 jours.
- **Expiration Grace Period** (Période de grâce de l'expiration) : définissez le nombre de jours pendant lesquels un utilisateur doit changer de mot de passe après l'expiration de ce dernier, entre 0 et 9999. La valeur par défaut est de 3 jours.
- **Password Reuse Interval** (Intervalle de réutilisation du mot de passe) : définissez le nombre de jours avant de pouvoir réutiliser un mot de passe, entre 1 et 365. La valeur par défaut est de 15 jours. Si vous activez le **History Count** (Nombre de l'historique) et le **Password Reuse Interval** (Intervalle de réutilisation du mot de passe), les deux exigences doivent être respectées. Par exemple, si vous définissez la limite de l'historique à 3 et l'intervalle de réutilisation à 10 jours, vous pouvez modifier votre mot de passe uniquement après 10 jours et après avoir modifié votre mot de passe trois fois.

Étape 4 Cliquez sur **Save** (Enregistrer).

Historique des paramètres de Gestionnaire de châssis

Fonctionnalités	Version	Détails
Améliorations des mots de passe utilisateur	9.13(1)	Nous avons ajouté des améliorations à la sécurité des mots de passe, notamment les éléments suivants : • Les mots de passe des utilisateurs peuvent comporter jusqu'à 127 caractères. L'ancienne limite était de 80 caractères. • La vérification de la robustesse du mot de passe est activée par défaut. • Une invite pour définir le mot de passe admin. • L'expiration du mot de passe. • Limite de réutilisation des mots de passe, Écrans nouveaux ou modifiés : • **System (Système)** > **User Management (Gestion des utilisateurs)** > **Local Users (Utilisateurs locaux)** • **System (Système)** > **User Management (Gestion des utilisateurs)** > **Settings (Paramètres)**
Prise en charge de l'authentification NTP sur le châssis Firepower 2100	9.10(1)	Vous pouvez maintenant configurer l'authentification du serveur NTP SHA1 dans FXOS. Écrans nouveaux ou modifiés de gestionnaire de châssis : **Platform Settings (Paramètres de la plateforme)** > **NTP** > **case à cocher Server Authentication : Enable (Authentification du serveur : activer)**, champ **Authentication Key** (Clé d'authentification), champ **Authentication Value** (Valeur d'authentification)

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.