



Gestion du périphérique

Ce guide s'applique à un Cisco Secure Firewall Management Center *local*, soit en tant que votre gestionnaire principal, soit en tant que gestionnaire affecté uniquement à l'analyse. Lorsque vous utilisez Cisco Defense Orchestrator (CDO) Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) en tant que gestionnaire principal, vous pouvez utiliser un centre de gestion local à des fins d'analyse uniquement. N'utilisez pas ce guide pour la gestion de CDO. voir [Gérer Firewall Threat Defense avec Cisco Cloud-Delivered Firewall Management Center dans Cisco Defense Orchestrator](#).

Ce chapitre décrit comment et gérer des périphériques dans Cisco Secure Firewall Management Center.

- [Connexion à l'interface de ligne de commande \(CLI\) sur le périphérique, à la page 1](#)
- [Ajouter un groupe de périphériques, à la page 3](#)
- [Arrêter ou redémarrer le périphérique, à la page 4](#)
- [Configurer les paramètres des périphériques, à la page 5](#)
- [Échange à chaud d'un SSD sur Cisco Secure Firewall, à la page 69](#)

Connexion à l'interface de ligne de commande (CLI) sur le périphérique

Vous pouvez vous connecter directement à l'interface de ligne de commande sur les périphériques défense contre les menaces. S'il s'agit de votre première connexion, terminez le processus de configuration initiale en utilisant l'utilisateur **admin** par défaut. voir [Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande](#).



Remarque Après qu'un utilisateur ait échoué à trois reprises à se connecter à l'interface de ligne de commande au moyen de SSH, le périphérique met fin à la connexion SSH.

Avant de commencer

Créez des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide de la commande **configure user add**.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande défense contre les menaces , à partir du port de console ou à l'aide de SSH.

Vous pouvez vous connecter en SSH à l'interface de gestion de l'appareil défense contre les menaces . Vous pouvez également vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface pour les connexions SSH. L'accès SSH aux interfaces de données est désactivé par défaut. Consultez [Secure Shell](#) pour autoriser les connexions SSH à des interfaces de données spécifiques.

Pour les périphériques physiques, vous pouvez vous connecter directement au port de console du périphérique. Consultez le guide du matériel de votre appareil pour en savoir plus sur le câble de la console. Utilisez les paramètres de série suivants :

- 9 600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

L'interface de ligne de commande sur le port de console est FXOS (à l'exception de l'ISA 3000, où il s'agit de l'interface de commande en ligne défense contre les menaces normale). Utilisez l'interface de ligne de commande de défense contre les menaces pour la configuration de base, la surveillance et le dépannage normal du système. Consultez la documentation de FXOS pour obtenir des renseignements sur les commandes FXOS.

Étape 2 Connectez-vous avec le nom d'utilisateur et le mot de passe **d'administrateur**.

Exemple :

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Étape 3 Si vous avez utilisé le port de console, accédez à l'interface de ligne de commande défense contre les menaces

connect ftd

Remarque Cette étape ne s'applique pas à ISA 3000.

Exemple :

```
firepower# connect ftd
>
```

Étape 4 À l'invite de l'interface de ligne de commande (>), utilisez l'une des commandes autorisées par votre niveau d'accès à la ligne de commande.

Pour revenir à FXOS sur le port de console, saisissez **exit**.

Étape 5 (Facultatif) Si vous avez utilisé SSH, vous pouvez vous connecter à FXOS.

connect fxos

Pour revenir à l'interface de ligne de commande défense contre les menaces , saisissez **exit**.

Étape 6 (Facultatif) Accédez à l'interface de ligne de commande de dépiage :

system support diagnostic-cli

Utilisez cette interface de ligne de commande pour un dépannage avancé. Cette interface de ligne de commande comprend des commandes supplémentaires **show** et d'autres commandes.

Elle comporte deux sous-modes : le mode EXEC utilisateur et le mode EXEC privilégié. Davantage de commandes sont disponibles en mode EXEC privilégié. Pour passer en mode d'exécution privilégié, saisissez la commande **enable** ; appuyez sur Entrée sans saisir de mot de passe lorsque vous y êtes invité.

Exemple :

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

Pour revenir à l'interface de ligne de commande classique, tapez **Ctrl-a, d**.

Ajouter un groupe de périphériques

Le centre de gestion vous permet de regrouper des périphériques afin de pouvoir déployer facilement des politiques et installer les mises à jour sur plusieurs périphériques. Vous pouvez développer et réduire la liste des périphériques du groupe.

Dans un déploiement multidomaine, vous pouvez créer des groupes de périphériques dans un domaine descendant uniquement. Lorsque vous configurez un Cisco Secure Firewall Management Center pour la multilocation, les groupes de périphériques existants sont supprimés. Vous pouvez les rajouter au niveau du domaine descendant.

Si vous ajoutez le périphérique principal d'une paire à haute disponibilité à un groupe, les deux périphériques sont ajoutés au groupe. Si vous rompez la paire à haute disponibilité, les deux périphériques restent dans ce groupe.

Procédure

Étape 1 Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.


Étape 2 Dans le menu déroulant **Add** (ajouter), choisissez **Add Group** (ajouter un groupe).

Pour modifier un groupe existant, cliquez sur **Edit** (✎) à côté du groupe que vous souhaitez modifier.

Étape 3 Saisissez un **Nom**.

Étape 4 Sous les **périphériques disponibles**, choisissez un ou plusieurs périphériques à ajouter au groupe de périphériques. Utilisez la touche Ctrl ou la touche Maj tout en cliquant pour choisir plusieurs périphériques.

Étape 5 Cliquez sur **Add** (ajouter) pour inclure les périphériques que vous avez choisis dans le groupe de périphériques.

- Étape 6** Éventuellement, pour supprimer un périphérique du groupe de périphériques, cliquez sur **Supprimer** () à côté du périphérique que vous souhaitez supprimer.
- Étape 7** Cliquez sur **OK** pour ajouter le groupe de périphériques.

Arrêter ou redémarrer le périphérique




Il est important que vous éteigniez votre système correctement. Débrancher l'alimentation ou appuyer sur le commutateur d'alimentation peut gravement endommager le système de fichiers. N'oubliez pas que de nombreux processus s'exécutent en permanence en arrière-plan, et que le fait de débrancher ou de couper l'alimentation ne permet pas l'arrêt en douceur de votre pare-feu.

Consultez la tâche suivante pour arrêter ou redémarrer votre système correctement.



Remarque Après le redémarrage de votre périphérique, vous pourriez voir un message d'erreur indiquant que la connexion de gestion n'a pas pu être rétablie. Dans certains cas, la connexion est tentée avant que l'interface de gestion sur le périphérique soit prête. La connexion fera l'objet d'une nouvelle tentative automatiquement et devrait s'établir dans les 15 minutes.

Procédure

- Étape 1** Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.
- Étape 2** À côté du périphérique que vous souhaitez redémarrer, cliquez sur **Edit** ().
- Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.
- Étape 3** Cliquez sur **Device (périphérique)**.
- Étape 4** Pour redémarrer le périphérique :
- Cliquez sur **Redémarrer l'appareil** ().
 - Lorsque vous y êtes invité, confirmez que vous souhaitez éteindre le périphérique.
- Étape 5** Pour éteindre le périphérique :
- Cliquez sur **Arrêt du périphérique** () dans la section **Système**.
 - Lorsque vous y êtes invité, confirmez que vous souhaitez éteindre le périphérique.
 - Si vous disposez d'une connexion de console au pare-feu, surveillez les notifications du système lorsque le pare-feu s'éteint. La notification suivante s'affichera :

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Si vous n'avez pas de connexion de console, attendez environ 3 minutes pour vous assurer que le système s'est éteint.

Pour l'ISA 3000, une fois l'arrêt terminé, le voyant DEL System s'éteint. Attendez au moins 10 secondes avant de retirer l'alimentation.

Configurer les paramètres des périphériques

La page **Devices (Périphériques) > Device Management (Gestion des périphériques)** fournit un éventail d'informations et d'options :

- **View By (afficher par)** : utilisez cette option pour afficher les périphériques en fonction du groupe, des licences, du modèle, de la version ou de la politique de contrôle d'accès.
- **Device State (état du périphérique)** : vous pouvez également afficher les périphériques en fonction de leur état. Vous pouvez cliquer sur l'icône d'un état pour afficher les périphériques qui lui sont associés. Le nombre de périphériques correspondant aux états est fourni entre parenthèses.
- **Search (rechercher)** : vous pouvez rechercher un périphérique configuré en fournissant son nom, le nom d'hôte ou l'adresse IP.
- **Ajouter des options** : vous pouvez ajouter des périphériques, des paires à haute disponibilité, des grappes et des groupes.
- **Edit and other actions (modifier et autres actions)** : utilisez l'icône **Edit** (✎) pour chaque périphérique configuré pour modifier les paramètres et les attributs du périphérique. Cliquez sur l'icône **Plus** (⋮) et exécutez d'autres actions :
 - **Access Control Policy (politique de contrôle d'accès)** : cliquez sur le lien dans la colonne Access Control Policy (politique de contrôle d'accès) pour afficher la politique déployée sur le périphérique.
 - **Delete** : pour annuler l'enregistrement du périphérique.
 - **Packet Tracer (Traceur de paquets)** : pour accéder à la page de Packet Tracer afin d'examiner la configuration de politique sur le périphérique en injectant un paquet de modèle dans le système.
 - **Packet Capture (Capture de paquets)** : pour accéder à la page de capture de paquets, où vous pouvez afficher les verdicts et les actions que le système prend lors du traitement d'un paquet.
 - **Revert Upgrade (annuler la mise à niveau)** : pour annuler les modifications de mise à niveau et de configuration effectuées après la dernière mise à niveau. Cette action permet de restaurer la version du périphérique avant la mise à niveau.
 - **Health Monitor (surveillance de l'intégrité)** : pour accéder à la page de surveillance de l'intégrité du périphérique.
 - **Troubleshooting Files (fichiers de dépannage)** : génère des fichiers de dépannage dans lesquels vous pouvez choisir le type de données à inclure dans le rapport.
 - Pour les périphériques de série Firepower 4100/9300, un lien vers l'interface Web gestionnaire de châssis.

Lorsque vous cliquez sur le périphérique, la page de propriétés du périphérique s'affiche avec plusieurs onglets. Vous pouvez utiliser les onglets pour afficher les informations sur le périphérique et configurer le routage, les interfaces, les ensembles en ligne et DHCP.

Modifier les paramètres généraux

La section **General (Généralités)** de la page **Device (Périphérique)** affiche les informations décrites dans le tableau ci-dessous.

Illustration 1 : Généralités

General	
Name:	Thing1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
Performance Profile:	Default
TLS Crypto Acceleration:	Disabled
Device Configuration:	<input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Download"/>

Tableau 1 : Champs du tableau de la section Généralités

Champ	Description
Nom	Le nom d'affichage du périphérique dans centre de gestion.
Transférer des paquets	Indique si le périphérique gère l'envoi ou non des paquets de données avec les événements à centre de gestion.
Mode	affiche le mode de l'interface de gestion pour le périphérique : roulage ou transparent .
Mode de conformité	Cela affiche la conformité des certifications de sécurité pour un périphérique. Les valeurs valides sont CC, UCAPL et Aucun.
Profil de rendement	Cette option affiche le profil de rendement d'allocation de ressources principales pour le périphérique, tel que configuré dans la politique des paramètres de la plateforme.
Accélération du chiffrement TLS :	Indique si l'accélération cryptographique TLS est activée ou désactivée.
Configuration du périphérique	Vous permet de copier, d'exporter ou d'importer une configuration. Consultez Copier une configuration sur un autre périphérique, à la page 7 et Exporter et importer la configuration du périphérique, à la page 8 .

Vous pouvez modifier certains de ces paramètres à partir de cette section.

Procédure

- Étape 1** Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.
- Étape 2** À côté du périphérique que vous souhaitez modifier, cliquez sur **Edit** (✎).
- Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.
- Étape 3** Cliquez sur **Device (périphérique)**.
- Étape 4** Dans la section **Général**, cliquez sur **Edit** (✎).
- Saisissez un **Name** (nom) pour le périphérique géré.
 - Cochez **Transférer les paquets** pour permettre le stockage des paquets de données avec des événements sur centre de gestion.
 - Cliquez sur **Force Deploy** pour forcer le déploiement des politiques et de la configuration de périphérique actuelles sur le périphérique.
- Remarque** Le déploiement forcé prend plus de temps que le déploiement normal, car il implique la génération complète des règles de politique à déployer sur défense contre les menaces .
- Étape 5** Pour les actions de **configuration des périphériques**, voir [Copier une configuration sur un autre périphérique, à la page 7](#) et [Exporter et importer la configuration du périphérique, à la page 8](#).
- Étape 6** Cliquez sur **Deploy** (Déployer).
-

Prochaine étape

- Déployer les changements de configuration.

Copier une configuration sur un autre périphérique

Lorsqu'un nouveau périphérique est déployé dans le réseau, vous pouvez facilement copier les configurations et les politiques à partir d'un périphérique préconfiguré, plutôt que de reconfigurer manuellement le nouveau périphérique.

Avant de commencer

Vérifiez que :

- Les périphériques source et destination défense contre les menaces sont du même modèle et exécutent la même version du logiciel.
- La source est soit un périphérique Cisco Secure Firewall Threat Defense autonome, soit une paire à haute disponibilité Cisco Secure Firewall Threat Defense.
- L'appareil de destination est un périphérique défense contre les menaces.
- Les périphériques source et de destination défense contre les menaces ont le même nombre d'interfaces physiques.
- Les périphériques source et de destination défense contre les menaces sont dans le même mode de pare-feu - routé ou transparent.

- Les périphériques source et destination défense contre les menaces sont dans le même mode de conformité des certifications de sécurité.
- Les périphériques source et de destination défense contre les menaces sont dans le même domaine,
- Le déploiement de la configuration n'est pas en cours sur les périphériques source ou de destination défense contre les menaces.

Procédure

Étape 1 Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.

Étape 2 À côté du périphérique que vous souhaitez modifier, cliquez sur **Edit** (✎).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Dans la section **General** (Général), effectuez l'une des opérations suivantes :

- Cliquez sur **Obtenir la configuration de l'appareil** (⬇️) pour copier la configuration de périphérique d'un autre périphérique vers le nouveau périphérique. Sur la page **Get Device Configuration** (obtenir la configuration du périphérique), sélectionnez le périphérique source dans la liste déroulante **Select Device** (sélectionner un périphérique).
- Cliquez sur **Pousser la configuration de l'appareil** (⬆️) pour copier la configuration de périphérique du périphérique actuel vers le nouveau. Dans la page **Push Device Configuration** (Envoyer la configuration de périphérique), sélectionnez la destination vers laquelle la configuration doit être copiée dans la liste déroulante **Target Device** (Périphérique cible).

Étape 5 (Facultatif) Cochez la case **Inclure la configuration des politiques partagées** pour copier les politiques.

Les politiques partagées comme la politique de CA, la NAT, les paramètres de plateforme et les politiques FlexConfig peuvent être partagées sur plusieurs périphériques.

Étape 6 Cliquez sur **OK**.

Vous pouvez surveiller l'état de la tâche de copie de la configuration du périphérique dans l'onglet **Tâches** du centre de messages.

Lorsque la tâche de copie de la configuration du périphérique est lancée, la configuration sur la machine cible est effacée et la configuration du périphérique source est copiée sur le périphérique de destination.



Avertissement Lorsque vous avez terminé la tâche de copie de la configuration du périphérique, vous ne pouvez pas rétablir la configuration d'origine de la machine cible.

Exporter et importer la configuration du périphérique

Vous pouvez exporter toute la configuration spécifique au périphérique configurable dans les pages Device (Périphériques), y compris :

- Interfaces
- Ensembles en ligne
- Routage
- DHCP (protocole de configuration dynamique des hôtes)
- VTEP
- Objets associés

Vous pouvez ensuite importer la configuration enregistrée pour le même périphérique dans les cas d'utilisation suivants :

- Déplacement du périphérique vers un autre centre de gestion- Il faut d'abord supprimer le périphérique du centre de gestion d'origine, puis l'ajouter au nouveau centre de gestion. Vous pouvez ensuite importer la configuration sauvegardée.
- Déplacement du périphérique entre les domaines : lorsque vous déplacez un périphérique entre les domaines, certaines configurations spécifiques au périphérique ne sont pas conservées car les objets de support (tels que les groupes d'interface pour les zones de sécurité) n'existent pas dans le nouveau domaine. En important la configuration après le déplacement du domaine, tous les objets nécessaires sont créés pour ce domaine et la configuration du périphérique est restaurée.
- Restauration d'une ancienne configuration : si vous avez déployé des modifications qui ont eu un impact négatif sur le fonctionnement du périphérique, vous pouvez importer une copie de sauvegarde d'une configuration de travail connue afin de restaurer un état opérationnel antérieur.
- Réenregistrement d'un périphérique : si vous un périphérique du centre de gestion, mais que vous souhaitez ensuite le réinscrire, vous pouvez importer la configuration enregistrée.

Consultez les consignes suivantes :

- Vous ne pouvez importer la configuration que sur le même périphérique (l'UUID doit correspondre). Vous ne pouvez pas importer une configuration vers un autre périphérique, même s'il s'agit du même modèle.
- Ne changez pas la version en cours d'exécution sur le périphérique entre l'exportation et l'importation ; la version doit correspondre.
- Si un objet n'existe pas, il sera créé. Si un objet existe, mais que sa valeur est différente, voir ci-dessous :

Tableau 2 : Action d'importation d'objets

Scénario	Action d'importation
Il existe un objet portant le même nom et la même valeur	Réutiliser des objets existants

Scénario	Action d'importation
Il existe un objet portant le même nom mais ayant une valeur différente	<ul style="list-style-type: none"> Objets réseau et port - créer des substitutions d'objets pour ce périphérique. Consultez Mises en priorité d'objets. Objets d'interface - créer de nouveaux objets. Par exemple, si le type (zone de sécurité ou groupe d'interfaces) et le type d'interface (routée ou commutée, par exemple) ne correspondent pas, un nouvel objet est créé. Tous les autres objets - réutiliser les objets existants même si les valeurs sont différentes.
L'objet n'existe pas	Créer de nouveaux objets

Procédure

Étape 1 Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.

Étape 2 En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** (✎).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Exporter la configuration.

a) Dans la zone **Général**, cliquez sur **Exporter**.

Illustration 2 : Exporter la configuration du périphérique

General

Name: 192.168.0.197 FTDv

Transfer Packets: Yes

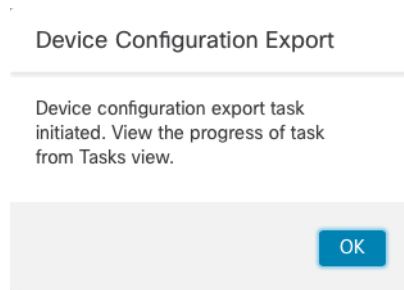
Mode: Routed

Compliance Mode: None

TLS Crypto Acceleration: Disabled

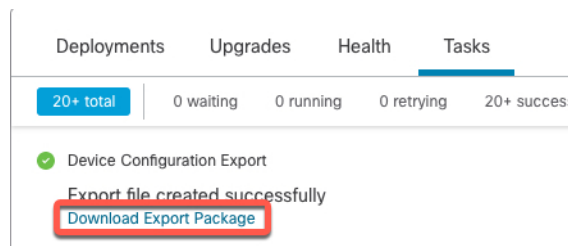
Device Configuration:

Vous êtes invité à confirmer l'exportation ; cliquez sur **OK**.

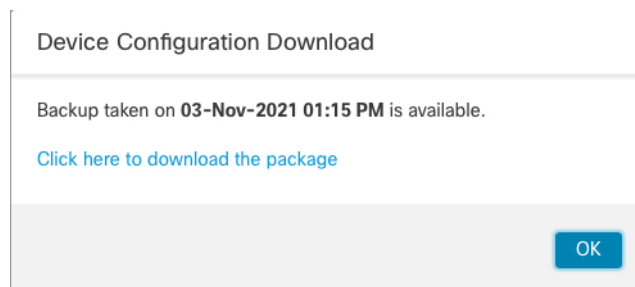
Illustration 3 : Confirmer l'exportation

Vous pouvez visualiser la progression de l'exportation dans la page **Tâches**.

- b) Sur la page **Notifications** > **Tâches**, assurez-vous que l'exportation est terminée ; cliquez sur **Télécharger le paquet d'exportation**. Vous pouvez également cliquer sur le bouton **Télécharger** dans la zone **Général**.

Illustration 4 : Exporter une tâche

Vous êtes invité à télécharger le paquet; cliquez sur **Cliquez ici pour télécharger le paquet** afin d'enregistrer le fichier localement, puis cliquez sur **OK** pour quitter la boîte de dialogue.

Illustration 5 : Télécharger le paquet

Étape 5 Importer la configuration.

- a) Dans la zone **Général**, cliquez sur **Importer**.

Illustration 6 : Importer la configuration du périphérique

General	
Name:	192.168.0.197 FTDv
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled
Device Configuration:	<input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Download"/>

Vous êtes invité à confirmer que la configuration actuelle sera remplacée. Cliquez sur **Oui**, puis accédez au paquet de configuration (avec le suffixe .sfo; notez que ce fichier est différent des fichiers de sauvegarde/restauration).

Illustration 7 : Importer un paquet

Device Configuration Import

This will replace current device configuration with new configuration from imported file. Do you want to continue?

Illustration 8 : Accéder au paquet

Name
 <input type="text" value="DeviceExport-0434ef00-15bb-11ec-bb94-93bde3ad19d.sfo"/>

Vous êtes invité à confirmer l'importation; cliquez sur **OK**.

Illustration 9 : Confirmer l'importation

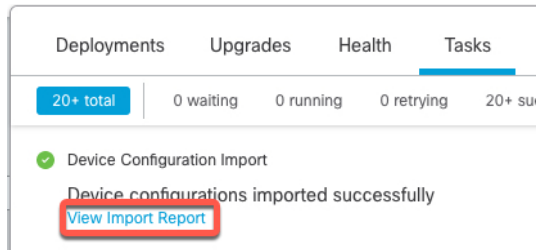
Device Configuration Import

Device configuration import task initiated. View the progress of task from Tasks view.

Vous pouvez visualiser la progression de l'importation dans la page **Tâches**.

- b) Consultez les rapports d'importation pour savoir ce qui a été importé. Sur la page **Notifications > Tâches**, cliquez sur **Afficher le rapport d'importation**.

Illustration 10 : Afficher le rapport d'importation



La page **Rapports d'importation de la configuration des périphériques** fournit des liens vers les rapports disponibles.

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bdde3ad19d	Report does not exist	Device configurations import report

Modifier les paramètres de licence

La section **Licence** de la page **Périphérique** affiche les licences activées pour le périphérique.

Vous pouvez activer des licences sur votre périphérique si vous possédez des licences disponibles sur votre centre de gestion.

Procédure

- Étape 1** Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.
- Étape 2** À côté du périphérique pour lequel vous souhaitez activer ou désactiver les licences, cliquez sur **Edit** (✎).
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.
- Étape 3** Cliquez sur **Device (périphérique)**.
- Étape 4** Dans la section **License** (licence), cliquez sur **Edit** (✎).
- Étape 5** Cochez ou décochez la case à côté de la licence que vous souhaitez activer ou désactiver pour le périphérique géré.
- Étape 6** Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Afficher les informations de base sur le système

La section **Système** de la page **Device** (Périphérique) affiche un tableau en lecture seule des informations système, comme décrit dans le tableau suivant.

Vous pouvez également éteindre ou redémarrer le périphérique.

Tableau 3 : Champs du tableau de section Système

Champ	Description
Modèle	Nom et numéro de modèle pour le périphérique géré.
Série	Le numéro de série du châssis de l'appareil géré.
Durée	L'heure système actuelle du périphérique.
Fuseau horaire	Affiche le fuseau horaire.
Version	La version du logiciel actuellement installée sur le périphérique géré.
Configuration des fuseaux horaires pour les règles basées sur le temps	L'heure système actuelle du périphérique, dans le fuseau horaire spécifié dans les paramètres de la plateforme du périphérique.

Afficher le moteur d'inspection

La section **Inspection Engine** (moteur d'inspection) de la page **Device** indique si votre appareil utilise Snort2 ou Snort3. Pour basculer le moteur d'inspection, consultez la section *Activer Snort 3 sur un périphérique individuel* dans [Guide de configuration Cisco Secure Firewall Management Center pour Snort 3](#).

Afficher les renseignements sur l'intégrité

La section **Health** (intégrité) de la page **Device** (Périphérique) affiche les informations décrites dans le tableau ci-dessous.

Tableau 4 : Champs du tableau de la section Health (Intégrité)

Champ	Description
État	Une icône qui représente l'état d'intégrité actuel du périphérique. Cliquez sur l'icône pour afficher le moniteur d'intégrité du périphérique.
Politique	Lien vers une version en lecture seule de la politique d'intégrité actuellement déployée sur le périphérique.
Exclu	Un lien vers la page d'exclusion de l'intégrité physique, où vous pouvez activer et désactiver les modules d'exclusion de l'intégrité.

Modifier les paramètres de gestion

Vous pouvez modifier les paramètres de gestion dans la zone **Management** (Gestion).

Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion

Si vous modifiez le nom d'hôte ou l'adresse IP d'un périphérique après l'avoir ajouté au centre de gestion (en utilisant la CLI du périphérique, par exemple), vous devez utiliser la procédure ci-dessous pour mettre à jour manuellement le nom d'hôte ou l'adresse IP sur l'interface de gestion centre de gestion

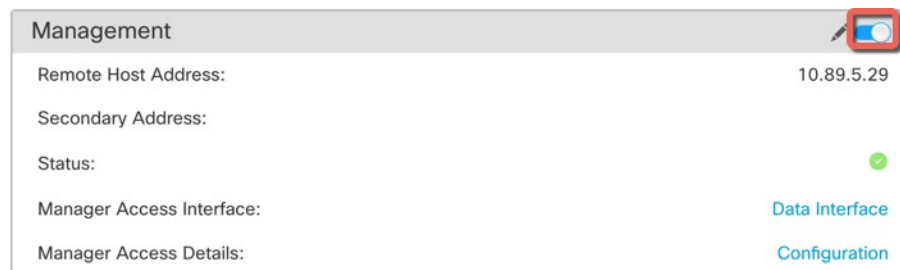
Pour modifier l'adresse IP de gestion des périphériques sur le périphérique, voir [Modifier les interfaces de gestion Défense contre les menaces au niveau de l'interface de ligne de commande](#), à la page 34.

Si vous avez utilisé uniquement l'ID NAT lors de l'enregistrement du périphérique, l'adresse IP affiche **NO-IP** sur cette page et vous n'avez pas besoin de mettre à jour l'adresse IP ni le nom d'hôte.

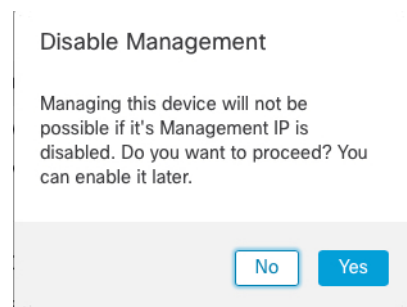
Procédure

- Étape 1** Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.
- Étape 2** À côté du périphérique dont vous souhaitez modifier les options de gestion, cliquez sur **Edit** (✎).
- Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.
- Étape 3** Cliquez sur **Device**(Périphériques) et affichez la zone **Management** (Gestion).
- Étape 4** Désactivez temporairement la gestion en cliquant sur le curseur pour la désactiver (🔴).

Illustration 11 : Désactiver la gestion



Vous êtes invité à procéder à la désactivation de la gestion; cliquez sur **Yes**(oui).



La désactivation de la gestion bloque la connexion entre le centre de gestion et le périphérique, mais n'annule **pas** l' de la suppression du périphérique à partir de centre de gestion.

Étape 5 Modifiez l'adresse IP de l' **distant** et l'**adresse secondaire** facultative (lors de l'utilisation d'une interface de données redondante) ou le nom d'hôte en cliquant sur **Edit** (✎).

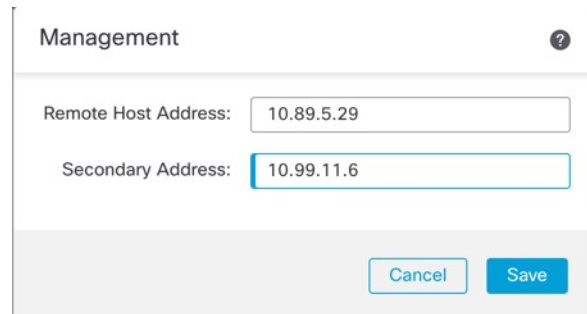
Illustration 12 : Modifier l'adresse de gestion



Étape 6 Dans la boîte de dialogue **Management** (gestion), modifiez le nom ou l'adresse IP dans le champ **Remote Host Address** (Adresse de l'hôte distant) (hôte) et le champ facultatif **Secondary Address** (adresse secondaire), puis cliquez sur **Save** (Enregistrer).

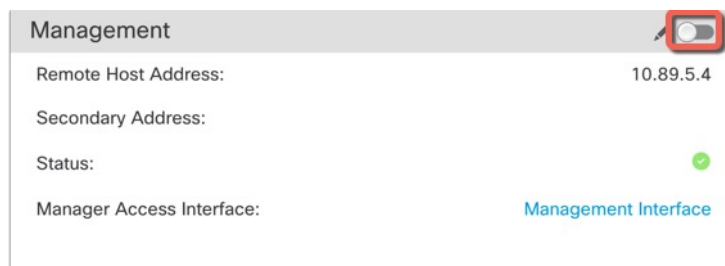
Pour en savoir plus sur l'utilisation d'une interface de données d'accès du gestionnaire secondaire, consultez [Configurer une interface de données d'accès du gestionnaire redondante](#), à la page 29.

Illustration 13 : Management IP Address (adresse IP de gestion)



Étape 7 Réactivez la gestion en cliquant sur le curseur pour l'activer (☑).

Illustration 14 : Activer la connexion de gestion



Modifier l'interface d'accès du gestionnaire de Management à Data (données)

Vous pouvez gérer la défense contre les menaces à partir de l'interface de gestion dédiée ou à partir d'une interface de données. Si vous souhaitez modifier l'interface d'accès du gestionnaire après avoir ajouté le périphérique à centre de gestion, suivez ces étapes pour migrer de l'interface de gestion vers une interface de données. Pour migrer dans l'autre sens, consultez [Modifier l'interface d'accès du gestionnaire de données à gestion, à la page 20](#).

Le fait d'initier la migration de l'accès du gestionnaire de la gestion vers les données entraîne centre de gestion à appliquer un blocage du déploiement à défense contre les menaces. Pour supprimer le blocage, activez l'accès du gestionnaire sur l'interface de données.

Consultez les étapes suivantes pour activer l'accès du gestionnaire sur une interface de données et configurer les autres paramètres requis.

Procédure

Étape 1

Initier la migration d'interface

- Sur la page **Devices(Périphériques) > Device Management (gestion des périphériques)**, cliquez sur **Edit** (✎) pour le périphérique.
- Passez à la section **Device > Management** (gestion des périphériques), puis cliquez sur le lien **Manager Access Interface** (Interface d'accès du gestionnaire) (Interface d'accès FMC).

Le champ **Manager Access Interface** (interface d'accès du gestionnaire) (Interface d'accès FMC) affiche l'interface de gestion actuelle. Lorsque vous cliquez sur le lien, choisissez le nouveau type d'interface, **Data Interface** (interface de données), dans la liste déroulante **Manage Device by** (gestion du périphérique par).

Illustration 15 : Interface d'accès du gestionnaire

Manager Access Interface

This is an advanced setting and need to be configured only if needed. See the [online help](#) for detailed steps.

Manage device by

Data Interface

Switching the manager access interface from Management to Data interface causes the deployment to be blocked. To unblock the deploy, pick a data interface and enable it for manager Access. See the [online help](#) for detailed steps.

Close Save

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

Vous devez maintenant effectuer les étapes restantes de cette procédure pour activer l'accès du gestionnaire sur l'interface de données. La zone **Management** affiche maintenant **Interface d'accès du gestionnaire : interface de données**, et **Détails d'accès du gestionnaire : Configuration**.

Illustration 16 : Accès du gestionnaire



Si vous cliquez sur **Configuration**, la boîte de dialogue **Accès du gestionnaire - Détails de la configuration** s'ouvre. Le **Mode d'accès du gestionnaire** affiche un état de déploiement en attente.

Étape 2

Activez l'accès de gestionnaire sur une interface de données sur la page **Périphériques > Gestion des périphériques > Interfaces > Modifier l'interface physique > Accès du gestionnaire**.

Voir [Configurer les interfaces en mode routé](#). Vous pouvez activer l'accès de gestionnaire sur une interface de données routées, ainsi qu'une interface secondaire facultative. Assurez-vous que ces interfaces sont entièrement configurées avec un nom et une adresse IP et qu'elles sont activées.

Si vous utilisez une interface secondaire à des fins de redondance, consultez [Configurer une interface de données d'accès du gestionnaire redondante](#), à la page 29 pour connaître la configuration supplémentaire requise.

Étape 3

(Facultatif) Si vous utilisez DHCP pour l'interface, activez la méthode DDNS de type Web sur la page **Périphériques > Gestion des périphériques > DHCP > DDNS**.

Voir [Configuration du DNS dynamique](#). Le DDNS s'assure que centre de gestion peut atteindre le défense contre les menaces à son nom de domaine complet (FQDN) si l'adresse IP de FTD change.

Étape 4

Assurez-vous que défense contre les menaces peut être acheminé vers centre de gestion par l'interface de données; Ajoutez une voie de routage statique, au besoin, sur **Périphériques > Gestion des périphériques > Routage > Routage statique**.

Consultez [Ajouter une route statique](#).

Étape 5

(Facultatif) Configurez le DNS dans une politique de paramètres de plateforme et appliquez-le à ce périphérique dans **Périphériques > Paramètres de la plateforme > DNS**.

Voir [DNS](#). Le DNS est requis si vous utilisez DDNS. Vous pouvez également utiliser le DNS pour les noms de domaine complets dans vos politiques de sécurité.

Étape 6

(Facultatif) Activez SSH pour l'interface de données dans une politique de paramètres de plateforme et appliquez-le à ce périphérique dans **Périphériques > Paramètres de la plateforme > Secure Shell**.

Voir [Secure Shell](#). SSH n'est pas activé par défaut sur les interfaces de données, donc si vous souhaitez gérer défense contre les menaces à l'aide de ce dernier, vous devez l'autoriser explicitement.

Étape 7

Déployer les changements de configuration.

Le centre de gestion déploiera les modifications de configuration sur l'interface de gestion actuelle. Après le déploiement, l'interface de données est maintenant prête à l'emploi, mais la connexion de gestion d'origine à l'interface de gestion est toujours active.

Étape 8

Au niveau de l'interface de ligne de commande défense contre les menaces (de préférence à partir du port de console), définissez l'interface de gestion pour utiliser une adresse IP statique et définissez la passerelle pour utiliser les interfaces de données.

configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces

- **ip_address netmask** : bien que vous ne prévoyiez pas utiliser l'interface de gestion, vous devez définir une adresse IP statique, par exemple une adresse privée pour pouvoir définir la passerelle sur **data-interfaces** (interfaces de données) (voir la puce suivante). Vous ne pouvez pas utiliser DHCP, car la voie de routage par défaut, qui doit être **data-interfaces**, pourrait être remplacée par une autre reçue du serveur DHCP.
- **data-interfaces** : ce paramètre fait passer le trafic de gestion sur le fond de panier afin qu'il puisse être distribué au moyen de l'interface de données d'accès du gestionnaire.

Nous vous recommandons d'utiliser le port de console au lieu d'une connexion SSH, car lorsque vous modifiez les paramètres réseau de l'interface de gestion, votre session SSH est déconnectée.

Étape 9

Au besoin, rebranchez le câblage de défense contre les menaces de sorte qu'il puisse atteindre le centre de gestion sur l'interface de données.

Étape 10

dans centre de gestion, désactivez la connexion de gestion, mettez à jour l'**adresse de l'hôte distant** Adresse IP et l'**Adresse secondaire** facultative pour défense contre les menaces à la section **Périphériques > Gestion des périphériques > Périphériques > Gestion** et réactivez la connexion.

Consultez [Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 15](#). Si vous avez utilisé le nom d'hôte défense contre les menaces ou simplement l'ID NAT lorsque vous avez ajouté défense contre les menaces à centre de gestion, vous n'avez pas besoin de mettre à jour la valeur; cependant, vous devez désactiver et réactiver la connexion de gestion pour redémarrer la connexion.

Étape 11

Vérifiez que la connexion de gestion a été rétablie.

Dans le centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils) > Device Management (gestion de l'appareil) > Device (appareil) > Management (gestion) > Manager Access - Configuration Details (accès du gestionnaire - Détails de la configuration) > Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces, entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

L'état suivant montre une connexion réussie pour une interface de données, en affichant l'interface « tap_nlp » interne.

Illustration 17 : Connection Status (état de la connexion)

Manager access - Configuration Details

Manager access configuration on device is in sync with the manager.

Configuration CLI Output **Connection Status**

sftunnel-status-brief command output from Firewall Threat Defense [\[Refresh \]](#)

```
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

[Close](#)

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez [Résoudre les problèmes de connectivité de gestion sur l'interface de données](#), à la page 45.

Modifier l'interface d'accès du gestionnaire de données à gestion

Vous pouvez gérer les défense contre les menaces à partir de l'interface de gestion dédiée ou à partir d'une interface de données. Si vous souhaitez modifier l'interface d'accès du gestionnaire après avoir ajouté le périphérique à centre de gestion, procédez comme suit pour migrer une interface de données vers l'interface de gestion. Pour migrer dans l'autre sens, consultez [Modifier l'interface d'accès du gestionnaire de Management à Data \(données\)](#), à la page 17.

Le lancement de la migration de l'accès au gestionnaire des données à la gestion amène centre de gestion à appliquer un blocage sur le déploiement à défense contre les menaces . Vous devez désactiver l'accès du gestionnaire sur l'interface de données pour supprimer le blocage.

Consultez les étapes suivantes pour désactiver l'accès du gestionnaire sur une interface de données et configurer les autres paramètres requis.

Procédure

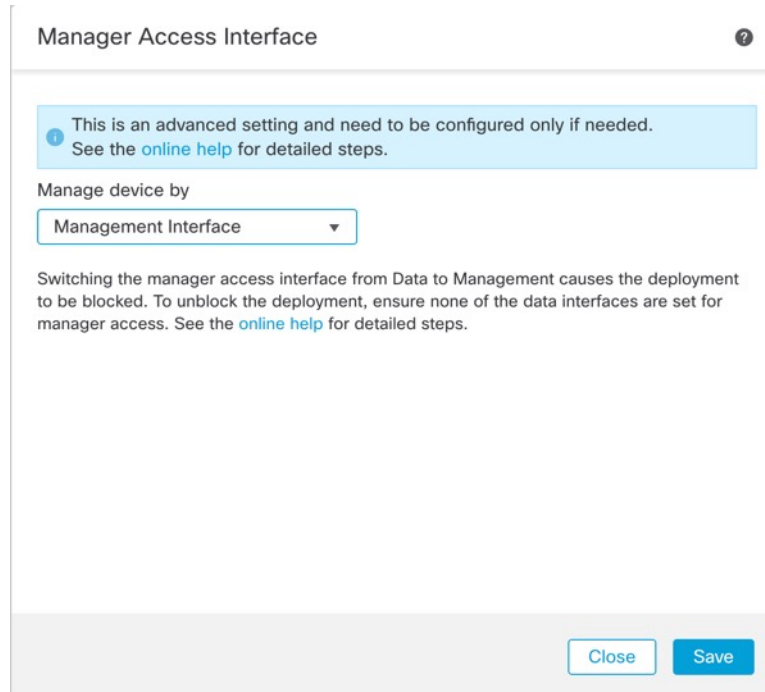
Étape 1

Initier la migration d'interface

- Sur la page **Devices(Périphériques) > Device Management (gestion des périphériques)**, cliquez sur **Edit** (✎) pour le périphérique.
- Passez à la section **Device > Management** (gestion des périphériques), puis cliquez sur le lien **Manager Access Interface** (Interface d'accès du gestionnaire) (Interface d'accès FMC).

Le champ **Manager Access Interface** affiche l'interface de gestion actuelle sous forme de données. Lorsque vous cliquez sur le lien, choisissez le nouveau type d'interface, **Management Interface** (interface de gestion), dans la liste déroulante **Manage device by** (Gérer le périphérique par).

Illustration 18 : Interface d'accès du gestionnaire



- c) Cliquez sur **Save** (enregistrer).

Vous devez maintenant effectuer les étapes restantes de cette procédure pour activer l'accès de gestionnaire sur l'interface de gestion. La zone **gestion** affiche maintenant l'**interface d'accès du gestionnaire : Interface de gestion**, l' et les détails d'**accès du gestionnaire : configuration**.

Illustration 19 : Accès du gestionnaire



Si vous cliquez sur **Configuration**, la boîte de dialogue **Accès du gestionnaire - Détails de la configuration** s'ouvre. Le **Mode d'accès du gestionnaire** affiche un état de déploiement en attente.

Étape 2

Désactivez l'accès du gestionnaire sur la ou les interfaces de données sur la page **Périphériques > Gestion des périphériques > interfaces > Modifier les interfaces physiques > Accès du gestionnaire**.

Voir [Configurer les interfaces en mode routé](#). Cette étape supprime le blocage lors du déploiement.

Étape 3 Si vous ne l'avez pas encore fait, configurez les paramètres DNS pour l'interface de données dans une politique de paramètres de plateforme et appliquez-la à ce périphérique dans **Périphériques > Paramètres de la plateforme > DNS**.

Voir [DNS](#). Le déploiement centre de gestion qui désactive l'accès du gestionnaire sur l'interface de données supprimera toute configuration DNS locale. Si ce serveur DNS est utilisé dans une politique de sécurité, comme un nom de domaine complet dans une règle d'accès, vous devez réappliquer la configuration DNS à l'aide de centre de gestion.

Étape 4 Déployer les changements de configuration.

Le centre de gestion déploiera les modifications de configuration sur l'interface de données actuelle.

Étape 5 Au besoin, reconnectez le câblage de défense contre les menaces pour qu'il puisse atteindre le centre de gestion sur l'interface de gestion.

Étape 6 Au niveau de l'interface de ligne de commande défense contre les menaces, configurez l'adresse IP de l'interface de gestion et la passerelle à l'aide d'une adresse IP statique ou d'un protocole DHCP.

Lorsque vous avez configuré l'interface de données pour l'accès du gestionnaire à l'origine, la passerelle de gestion a été définie pour les interfaces de données, qui transmettent le trafic de gestion sur le fond de panier afin qu'il puisse être acheminé par l'interface de données d'accès du gestionnaire. Vous devez maintenant définir une adresse IP pour la passerelle sur le réseau de gestion.

Adresse IP statique

```
configure network {ipv4 | ipv6} manual ip_address netmask gateway_ip
```

DHCP:

```
configure network {ipv4 | ipv6} dhcp
```

Étape 7 Dans centre de gestion, désactivez la connexion de gestion, mettez à jour l'adresse de l'**distant**, puis supprimez l'**adresse secondaire** facultative pour le défense contre les menaces dans la section **Device > Management > Device > Management** (gestion des périphériques), puis réactivez la connexion.

Consultez [Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 15](#). Si vous avez utilisé le nom d'hôte défense contre les menaces ou simplement l'ID NAT lorsque vous avez ajouté défense contre les menaces à centre de gestion, vous n'avez pas besoin de mettre à jour la valeur; cependant, vous devez désactiver et réactiver la connexion de gestion pour redémarrer la connexion.

Étape 8 Vérifiez que la connexion de gestion a été rétablie.

Dans centre de gestion, vérifiez l'état de la connexion de gestion sur le champ **Périphériques > Gestion des périphériques > Périphérique > Gestion > État** ou affichez les notifications dans centre de gestion.

Dans l'interface de ligne de commande défense contre les menaces, entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez [Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 45](#).

Modifier l'interface d'accès du gestionnaire de Management à Data (données) dans une paire à haute disponibilité

Vous pouvez gérer le FTD à partir de l'interface de gestion dédiée ou à partir d'une interface de données. Si vous souhaitez modifier l'interface d'accès Cisco Defense Orchestrator après avoir ajouté le périphérique à CDO, suivez ces étapes pour migrer de l'interface de gestion vers une interface de données. Pour migrer dans l'autre sens, consultez [Modifier l'interface d'accès du gestionnaire de Data \(données\) à Management \(gestion\) dans une paire à haute disponibilité, à la page 26](#).

Le lancement de la migration de l'accès de la gestion aux données par CDO] fait en sorte que CDO applique un blocage sur le déploiement sur FTD. Pour supprimer le blocage, activez l'accès CDO sur l'interface de données.



Remarque Sauf indication contraire, effectuez toutes les étapes mentionnées dans cette section uniquement sur l'unité active. Une fois les modifications de configuration déployées, l'unité de secours synchronise la configuration et les autres informations d'état de l'unité active.

Consultez les étapes suivantes pour activer l'accès à CDO sur une interface de données et configurer les autres paramètres requis.

Avant de commencer

Prise en charge des modèles—Défense contre les menaces

Procédure

Étape 1

Initier la migration d'interface

- Dans la barre de navigation, cliquez sur **Inventaire**.
- Cliquez sur l'onglet **FTD**.
- Sélectionnez le périphérique actif et dans le volet **Management** (Management) à droite, cliquez sur **Device Summary** (résumé du périphérique).
- Dans la zone **Management** (gestion), cliquez sur le lien de **Manager Access Interface** (Interface d'accès du gestionnaire).

Le champ **Manager Access Interface** (interface d'accès du gestionnaire) affiche l'interface de gestion actuelle. Lorsque vous cliquez sur le lien, choisissez le nouveau type d'interface, **Data Interface** (interface de données), dans la liste déroulante **Manage Device by** (gestion du périphérique par).

Manager Access Interface

This is an advanced setting and need to be configured only if needed.
See the [online help](#) for detailed steps.

Manage device by

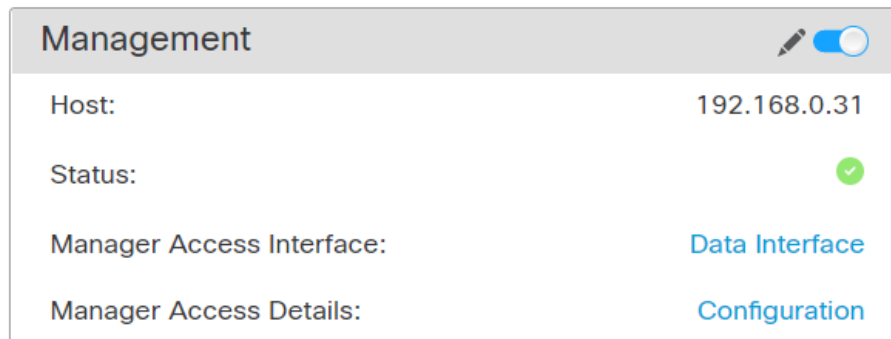
Data Interface

Remarque La liaison n'est pas disponible pour l'unité de secours, car l'interface d'accès peut être modifiée sur l'unité active.

e) Cliquez sur **Save** (enregistrer).

Vous devez maintenant effectuer les étapes restantes de cette procédure pour activer l'accès CDO sur l'interface de données. La zone **Gestion** affiche maintenant **Interface d'accès du gestionnaire : Interface de données**, et **Détails de l'accès au gestionnaire : Configuration**.

Illustration 20 : Accès du gestionnaire



Si vous cliquez sur **Configuration**, la boîte de dialogue **Accès du gestionnaire - Détails de la configuration** s'ouvre. Le **mode d'accès du gestionnaire** affiche un état de déploiement en attente.

Étape 2 Activer l'accès CDO à une interface de données sur la page **Devices > Device Management > Interfaces > Edit Physical Interface > Manager Access** (Périphériques > Gestion des périphériques > Interfaces > Modifier l'interface physique > Accès du gestionnaire).

Consultez la section [Configure Routed Mode Interfaces](#) (Configuration des interfaces en mode routé). Vous pouvez activer l'accès CDO sur une interface de données routée. Assurez-vous que cette interface est entièrement configurée avec un nom et une adresse IP et qu'elle est activée.

Étape 3 Assurez-vous que FTD peut acheminer vers le CDO par l'interface de données; Ajoutez une voie de routage statique, au besoin sur **Devices > Device Management > Routing > Static Route** (Périphériques > Gestion des périphériques > Routage > Routage statique).

Consultez [Ajouter une route statique](#).

Étape 4 (Facultatif) Configurez le DNS dans une politique de paramètres de plateforme et appliquez-le à ce périphérique dans **Périphériques > Paramètres de la plateforme > DNS**.

DNS. Le DNS est requis si vous utilisez DDNS. Vous pouvez également utiliser le DNS pour les noms de domaine complets dans vos politiques de sécurité.

Étape 5 (Facultatif) Activez SSH pour l'interface de données dans une politique de paramètres de plateforme et appliquez-le à ce périphérique dans **Périphériques > Paramètres de la plateforme > Secure Shell**.

Voir [Secure Shell](#). SSH n'est pas activé par défaut sur les interfaces de données, donc si vous souhaitez gérer FTD à l'aide de SSH, vous devez l'autoriser explicitement.

Étape 6 Déployer les changements de configuration.

Le CDO déploiera les modifications de configuration sur l'interface de gestion actuelle. Après le déploiement, l'interface de données est maintenant prête à l'emploi, mais la connexion de gestion d'origine à l'interface de gestion est toujours active.

Étape 7

Au niveau de l'interface de ligne de commande de FTD (de préférence à partir du port de console), réglez l'interface de gestion pour utiliser une adresse IP statique et réglez la passerelle pour utiliser les interfaces de données.

configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces

- **ip_address netmask** : bien que vous ne prévoyiez pas utiliser l'interface de gestion, vous devez définir une adresse IP statique, par exemple une adresse privée pour pouvoir définir la passerelle sur **data-interfaces** (interfaces de données) (voir la puce suivante).
- **data-interfaces** : ce paramètre transfère le trafic de gestion sur le fond de panier afin qu'il puisse être acheminé par l'interface de données d'accès CDO.

Nous vous recommandons d'utiliser le port de console au lieu d'une connexion SSH, car lorsque vous modifiez les paramètres réseau de l'interface de gestion, votre session SSH est déconnectée.

Remarque Répétez cette étape sur l'unité de secours.

Étape 8

Lorsque le déploiement est terminé à environ 90 %, la nouvelle interface de gestion prend effet. À ce stade, vous devez re-brancher le FTD de sorte que CDO atteigne FTD sur l'interface de données et termine le déploiement avec succès.

Après le re-câblage, le déploiement peut échouer s'il a expiré avant de rétablir la connexion de gestion à la nouvelle interface. Dans ce cas, vous devez relancer le déploiement après le recâblage pour un déploiement réussi.

Remarque Répétez cette étape sur l'unité de secours.

Étape 9

Vérifiez que la connexion de gestion a été rétablie.

Dans CDO, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils) > Device Management (gestion des appareils) > Device (appareil) > Management (gestion) > Manager Access - Configuration Details (Accès au gestionnaire - Détails de la configuration) > Connection Status (état de la connexion)**.

Au niveau de l'interface de ligne de commande FTD, entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

L'état suivant montre une connexion réussie pour une interface de données, en affichant l'interface « tap_nlp » interne.

Illustration 21 : Connection Status (état de la connexion)

Manager access - Configuration Details

Manager access configuration on device is in sync with the manager.

Configuration CLI Output **Connection Status**

sftunnel-status-brief command output from Firewall Threat Defense [Refresh]

```
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

[Close](#)

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez [Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 45](#).

Modifier l'interface d'accès du gestionnaire de Data (données) à Management (gestion) dans une paire à haute disponibilité

Vous pouvez gérer le FTD à partir de l'interface de gestion dédiée ou à partir d'une interface de données. Si vous souhaitez modifier l'interface d'accès Cisco Defense Orchestrator après avoir ajouté le périphérique à CDO, procédez comme suit pour migrer une interface de données vers l'interface de gestion. Pour migrer dans l'autre sens, consultez [Modifier l'interface d'accès du gestionnaire de Management à Data \(données\) dans une paire à haute disponibilité, à la page 23](#).

Le lancement de la migration de l'accès à CDO des données vers la gestion entraîne l'application d'un blocage par CDO du déploiement vers le FTD. Vous devez désactiver l'accès CDO sur l'interface de données pour supprimer le blocage.



Remarque

Sauf indication contraire, effectuez toutes les étapes mentionnées dans cette section uniquement sur l'unité active. Une fois les modifications de configuration déployées, l'unité de secours synchronise la configuration et les autres informations d'état de l'unité active.

Consultez les étapes suivantes pour désactiver l'accès CDO sur une interface de données et configurer les autres paramètres requis.

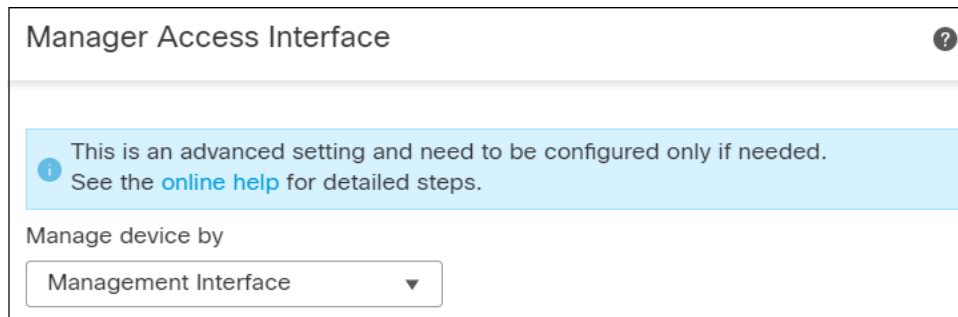
Procédure

Étape 1

Initier la migration d'interface

- a) Dans la barre de navigation, cliquez sur **Inventaire**.
- b) Cliquez sur l'onglet **FTD**.
- c) Sélectionnez le périphérique actif et dans le volet **Management** (Management) à droite, cliquez sur **Device Summary** (résumé du périphérique).
- d) Dans la zone **Management** (gestion), cliquez sur le lien de **Manager Access Interface** (Interface d'accès du gestionnaire).

Le champ **Manager Access Interface** (interface d'accès du gestionnaire) affiche l'interface de gestion actuelle sous forme de données. Lorsque vous cliquez sur le lien, choisissez le nouveau type d'interface, **Management Interface** (interface de gestion), dans la liste déroulante **Manage device by** (Gérer le périphérique par).

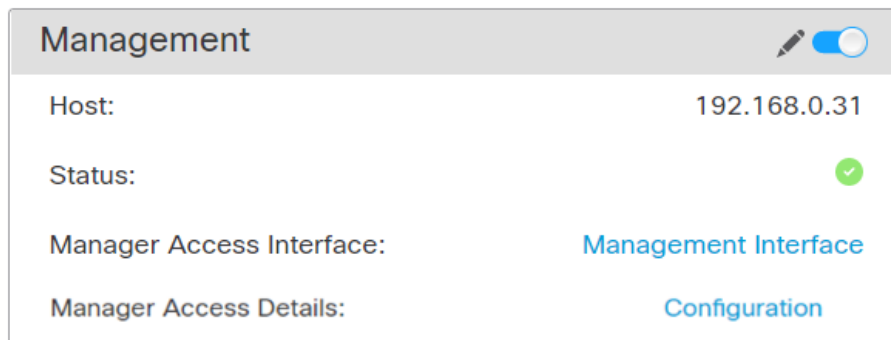


Remarque La liaison n'est pas disponible pour l'unité de secours, car l'interface d'accès peut être modifiée sur l'unité active.

- e) Cliquez sur **Save** (enregistrer).

Vous devez maintenant effectuer les étapes restantes de cette procédure pour activer l'accès CDO sur l'interface de données. La zone **Management** (gestion) affiche maintenant **Manager Access Interface: Management Interface** (Interface d'accès du gestionnaire : Interface de gestion) et **Manager Access Details: Configuration** (Détails de l'accès du gestionnaire : Configuration).

Illustration 22 : Accès du gestionnaire



Si vous cliquez sur **Configuration**, la boîte de dialogue **Accès du gestionnaire - Détails de la configuration** s'ouvre. Le **mode d'accès du gestionnaire** affiche un état de déploiement en attente.

- Étape 2** Désactivez l'accès CDO sur une interface de données sur la page des **périphériques > gestion des périphériques > interfaces > Modifier les interfaces physiques > Accès FMC**.
- Voir [Configurer les interfaces en mode routage](#). Cette étape supprime le blocage lors du déploiement.
- Étape 3** Si vous ne l'avez pas encore fait, configurez les paramètres DNS pour l'interface de données dans une politique de paramètres de plateforme et appliquez-la à ce périphérique dans **Périphériques > Paramètres de la plateforme > DNS**.
- Consultez [DNS](#). Le déploiement CDO qui désactive l'accès CDO sur l'interface de données supprimera toute configuration DNS locale. Si ce serveur DNS est utilisé dans une politique de sécurité, comme un nom de domaine complet dans une règle d'accès, vous devez réappliquer la configuration DNS à l'aide de CDO.
- Étape 4** Déployer les changements de configuration.
- Le CDO déploiera les modifications de configuration sur l'interface de données actuelle.
- Étape 5** Lorsque le déploiement est terminé à environ 90 %, la nouvelle interface de gestion prend effet. À ce stade, vous devez re-câbler FTD de sorte que CDO atteigne FTD sur l'interface de gestion et termine le déploiement avec succès.
- Après le re-câblage, le déploiement peut échouer s'il a expiré avant de rétablir la connexion de gestion à la nouvelle interface. Dans ce cas, vous devez relancer le déploiement après le recâblage pour un déploiement réussi.
- Remarque** Répétez cette étape sur l'unité de secours.
- Étape 6** Au niveau de l'interface de ligne de commande de FTD, configurez l'adresse IP de l'interface de gestion et la passerelle à l'aide d'une adresse IP statique ou d'un protocole DHCP.
- Lorsque vous avez configuré l'interface de données pour l'accès CDO à l'origine, la passerelle de gestion a été configurée pour les interfaces de données, qui transmettent le trafic de gestion sur le fond de panier pour qu'il puisse être acheminé par l'interface de données de l'accès CDO. Vous devez maintenant définir une adresse IP pour la passerelle sur le réseau de gestion.
- Adresse IP statique**
- ```
configure network {ipv4 | ipv6} manual ip_address netmask gateway_ip
```
- DHCP:**
- ```
configure network {ipv4 | ipv6} dhcp
```
- Remarque** Répétez cette étape sur l'unité de secours.
- Étape 7** Vérifiez que la connexion de gestion a été rétablie.
- Dans CDO, vérifiez l'état de la connexion de gestion sur le champ **Périphériques > Gestion des périphériques > Périphérique > Gestion > État** ou affichez les notifications dans CDO.
- Au niveau de l'interface de ligne de commande FTD, entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.
- S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez [Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 45](#).
-

Configurer une interface de données d'accès du gestionnaire redondante

Lorsque vous utilisez une interface de données pour l'accès de gestionnaire, vous pouvez configurer une interface de données secondaire pour prendre en charge les fonctions de gestion si l'interface principale tombe en panne. Vous ne pouvez configurer qu'une seule interface secondaire. Le périphérique utilise la surveillance ANS (Accord de niveau de service) pour suivre la viabilité des routes statiques et une zone ECMP qui contient les deux interfaces afin que le trafic de gestion puisse utiliser ces dernières.

Avant de commencer

- L'interface secondaire doit se trouver dans une zone de sécurité distincte de l'interface principale.
- L'ensemble des mêmes exigences s'appliquent à l'interface secondaire et à l'interface principale. Consultez [Utilisation de l'interface de données Défense contre les menaces pour la gestion](#).

Procédure

Étape 1 Sur la page **Devices(Périphériques) > Device Management (gestion des périphériques)**, cliquez sur **Edit** (✎) pour le périphérique.

Étape 2 Activez l'accès au gestionnaire pour l'interface secondaire.

Ce paramètre s'ajoute aux paramètres d'interface standard tels que l'activation de l'interface, la définition du nom, la définition de la zone de sécurité et la définition d'une adresse IPv4 statique.

- Choisissez **Interfaces > Edit Physical Interface (Modifier l'interface physique) > Manager Access (Accès au gestionnaire)**.
- Cochez **Enable management on this interface for the Manager** (Activer la gestion sur cette interface pour le gestionnaire).
- Cliquez sur **OK**.

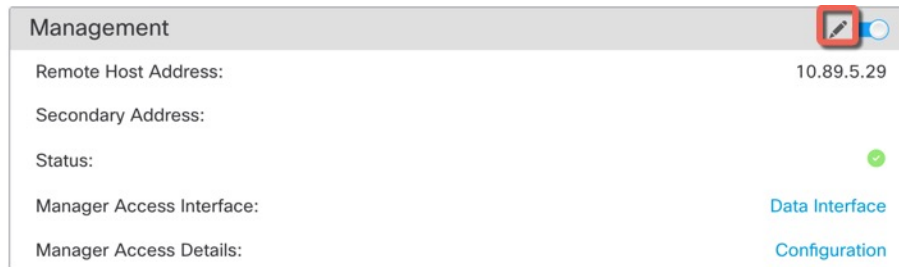
Les deux interfaces affichent (**Manager Access**) dans la liste des interfaces.

Illustration 23 : Liste des interfaces

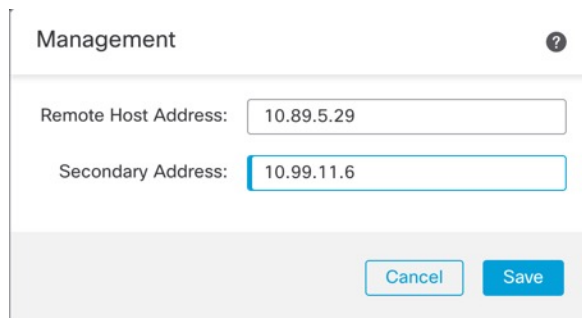
Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

Étape 3 Ajouter l'adresse secondaire aux paramètres de **gestion**.

- a) Cliquez sur **Device**(Périphériques) et affichez la zone **Management** (Gestion).
- b) Cliquez sur **Edit** (✎).

Illustration 24 : Modifier l'adresse de gestion

- c) Dans la boîte de dialogue **Management** (gestion), modifiez le nom ou l'adresse IP dans le champ **Secondary Address** (adresse secondaire).

Illustration 25 : Management IP Address (adresse IP de gestion)

- d) Cliquez sur **Save** (enregistrer).

Étape 4 Créez une zone ECMP avec les deux interfaces.

- a) Cliquez sur **Routing** (Routage).
- b) Dans la liste déroulante du routeur virtuel, choisissez le routeur virtuel dans lequel se trouvent les interfaces principale et secondaire.
- c) Cliquez sur **ECMP**, puis sur **Add** (Ajouter).
- d) Saisissez un **nom** pour la zone ECMP.
- e) Sélectionnez les interfaces principale et secondaire dans la zone **Interfaces disponibles**, puis cliquez sur **Add** (Ajouter).

Illustration 26 : Ajouter une zone ECMP

The screenshot shows a dialog box titled "Add ECMP". At the top right of the dialog are a help icon (question mark) and a close icon (X). Below the title bar is a text input field labeled "Name" containing the text "redundant-mgmt". The main area of the dialog is divided into two columns. The left column is titled "Available Interfaces" and is currently empty. The right column is titled "Selected Interfaces" and contains two entries: "outside" and "redundant", each with a trash icon to its right. A blue "Add" button is located between the two columns. At the bottom of the dialog are two buttons: "Cancel" and "OK".

f) Cliquez sur **OK**, puis sur **Save**(Enregistrer).

Étape 5

Ajoutez des routes statiques par défaut à coût égal pour les deux interfaces et activez le suivi SLA sur les deux.

Les routes doivent être identiques, à l'exception de la passerelle, et elles doivent toutes deux avoir la métrique 1. L'interface principale doit déjà avoir une voie de routage par défaut que vous pouvez modifier.

Illustration 27 : Ajouter/modifier un routage statique

Edit Static Route Configuration ?

Type: IPv4 IPv6

Interface*
outside

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Search

10.99.11.1
any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8

Add

Selected Network

any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway
10.89.5.1 +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

- Cliquez sur **Static Route** (Routage statique).
- Cliquez sur **Add Route** (Ajouter un routage) pour ajouter une nouvelle route ou cliquez sur **Edit** () pour une route existante.
- Choisissez une interface dans la liste déroulante **Interface**.
- Pour le réseau de destination, sélectionnez **any-ipv4** dans la zone des **réseaux disponibles** et cliquez sur **Ajouter**.
- Saisissez la **passerelle** par défaut.
- Pour le **suivi du routage**, cliquez sur **Ajouter** (+) pour ajouter un nouvel objet de moniteur SLA.
- Saisissez les paramètres requis, notamment les suivants :
 - L'**adresse du moniteur** comme adresse IP centre de gestion.
 - La zone de l'interface de gestion principale ou secondaire dans **Zones disponibles**; Par exemple, choisissez la zone externe pour l'objet d'interface principal et la zone de gestion pour l'objet d'interface secondaire.

Consultez [Surveillance SLA](#) pour obtenir de plus amples renseignements.

Illustration 28 : Ajouter un moniteur SLA

New SLA Monitor Object ?

Name:

Description:

Frequency (seconds):
(1-604800)

SLA Monitor ID*:

Threshold (milliseconds):
(0-60000)

Timeout (milliseconds):
(0-604800000)

Data Size (bytes):
(0-16384)

ToS:

Number of Packets:

Monitor Address*:

Available Zones

Selected Zones/Interfaces

- h) Cliquez sur **Save**(Enregistrer), puis choisissez l'objet SLA que vous venez de créer dans la liste déroulante **Route Tracking** (suivi de routage).
- i) Cliquez sur **OK**, puis sur **Save**(Enregistrer).
- j) Répétez l'opération pour la route par défaut pour l'autre interface de gestion.

Étape 6

Déployer les changements de configuration.

Dans le cadre du déploiement de cette fonctionnalité, le centre de gestion active l'interface secondaire pour le trafic de gestion, y compris la configuration de routage basée sur des règles générées automatiquement pour que le trafic de gestion atteigne la bonne interface de données. Le centre de gestion déploie également une deuxième instance de la commande **configure network management-data-interface**. Notez que si vous modifiez l'interface secondaire dans l'interface de gestion, vous ne pourrez pas configurer la passerelle ou

modifier la route par défaut, car la route statique de cette interface ne peut être modifiée que dans l'interface de gestion centre de gestion.

Modifier les interfaces de gestion Défense contre les menaces au niveau de l'interface de ligne de commande

Modifier les paramètres de l'interface de gestion sur le périphérique géré à l'aide de l'interface de ligne de commande. Bon nombre de ces paramètres sont ceux que vous avez définis lors de la configuration initiale; Cette procédure vous permet de modifier ces paramètres et de définir des paramètres supplémentaires tels que l'activation d'une interface d'événement si votre modèle la prend en charge ou l'ajout de routes statiques.



Remarque

Cette rubrique s'applique à l'interface de gestion dédiée. Vous pouvez également configurer une interface de données pour la gestion. Si vous souhaitez modifier les paramètres réseau pour cette interface, vous devez le faire dans centre de gestion et non au niveau de la CLI. Si vous devez dépanner une connexion de gestion interrompue et devez apporter des modifications directement à partir de défense contre les menaces , consultez [Modifier l'interface de données Défense contre les menaces utilisée pour la gestion au niveau de l'interface de ligne de commande](#), à la page 40.

Pour obtenir des informations détaillées sur l'interface de ligne de commande de défense contre les menaces , consultez [Référence des commandes de défense contre les menaces de Cisco Secure Firewall](#).



Remarque

Lorsque vous utilisez SSH, soyez prudent lorsque vous apportez des modifications à l'interface de gestion; Si vous ne pouvez pas vous reconnecter à cause d'une erreur de configuration, vous devrez accéder au port de console du périphérique.



Remarque

Si vous modifiez l'adresse IP de gestion du périphérique , consultez les tâches suivantes pour la connectivité centre de gestion en fonction de la façon dont vous avez identifié le centre de gestion lors de la configuration initiale du périphérique à l'aide de la commande **configure manager add** :

- **Adresse IP : aucune action.** Si vous avez identifié le centre de gestion utilisant une adresse IP accessible, la connexion de gestion sera rétablie automatiquement après plusieurs minutes. Nous vous recommandons de modifier également l'adresse IP du périphérique indiquée dans centre de gestion pour maintenir la synchronisation des informations. voir [Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 15](#). Cette action peut aider la connexion à se rétablir plus rapidement. **Remarque** : Si vous avez spécifié une adresse IP centre de gestion inaccessible, consultez la procédure pour l'ID NAT ci-dessous.
- **ID NAT uniquement : rétablissez manuellement la connexion.** Si vous avez identifié centre de gestion en utilisant uniquement l'ID NAT, la connexion ne peut pas être rétablie automatiquement. Dans ce cas, modifiez l'adresse IP de gestion du périphérique dans centre de gestion en fonction de [Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 15](#).



Remarque Dans une configuration à haute disponibilité centre de gestion, lorsque vous modifiez l'adresse IP de gestion à partir de l'interface de ligne de commande du périphérique ou à partir de centre de gestion, le centre de gestion secondaire ne reflète pas les modifications, même après une synchronisation à haute disponibilité. Pour vous assurer que le centre de gestion secondaire est également mis à jour, inversez les rôles entre les deux centre de gestion, de sorte que le centre de gestion secondaire devienne l'unité active. Modifiez l'adresse IP de gestion du périphérique enregistré sur la page de gestion des périphériques de centre de gestion désormais actif.

Avant de commencer

- Vous pouvez créer des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide la commande **configure user add** ; voir [Ajouter un utilisateur interne au niveau de l'interface de ligne de commande](#). Vous pouvez également configurer les utilisateurs AAA en fonction de [Authentification extérieure](#).

Procédure

Étape 1

Connectez-vous à l'interface de ligne de commande du périphérique, soit à partir du port de console ou à l'aide de SSH.

Étape 2

Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 3

(Firepower 4100/9300 uniquement) Activez la deuxième interface de gestion comme interface d'événements uniquement.

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

Vous avez toujours besoin d'une interface de gestion pour la gestion du trafic. Si votre appareil dispose d'une deuxième interface de gestion, vous pouvez l'activer pour le trafic d'événements uniquement.

Vous pouvez éventuellement désactiver les événements pour l'interface de gestion principale à l'aide de la commande **configure network management-interface disable-events-channel**. Dans les deux cas, le périphérique tentera d'envoyer des événements sur l'interface d'événements seulement et, si cette interface est en panne, il enverra des événements sur l'interface de gestion même si vous désactivez le canal d'événements.

Vous ne pouvez pas désactiver les canaux d'événement et de gestion sur une interface.

Pour utiliser une interface d'événements distincte, vous devez également activer une interface d'événements sur centre de gestion. Consultez la section [Guide d'administration Cisco Secure Firewall Management Center](#).

Exemple :

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

Étape 4

Configurez l'adresse IP de l'interface de gestion et/ou de l'interface d'événements :

Si vous ne spécifiez pas l'argument *management_interface*, vous modifiez les paramètres réseau de l'interface de gestion par défaut. Lors de la configuration d'une interface d'événements, veillez à spécifier l'argument *management_interface*. L'interface d'événements peut se trouver sur un réseau distinct de celui de l'interface de gestion ou sur le même réseau. Si vous êtes connecté à l'interface que vous configurez, vous serez déconnecté. Vous pouvez vous reconnecter à la nouvelle adresse IP.

a) Configurer l'adresse IPv4 :

- Configuration manuelle :

```
configure network ipv4 manual ip_address netmask gateway_ip [management_interface]
```

Notez que *gateway_ip* dans cette commande est utilisée pour créer la voie de routage par défaut pour le périphérique. Si vous configurez une interface d'événements uniquement, vous devez entrer *gateway_ip* dans la commande; cependant, cette entrée configure simplement la voie de routage par défaut à la valeur que vous spécifiez et ne crée pas de voie de routage statique distincte pour l'interface d'événement. Si vous utilisez une interface d'événements uniquement sur un réseau différent de l'interface de gestion, nous vous recommandons de définir *gateway_ip* à utiliser avec l'interface de gestion, puis de créer une voie de routage statique séparément pour l'interface d'événements uniquement à l'aide de la commande **configure network static-routes**.

Exemple :

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.
```

```
>
```

- DHCP (pris en charge sur l'interface de gestion par défaut uniquement) :

```
configure network ipv4 dhcp
```

b) Configurer l'adresse IPv6

- Autoconfiguration sans état

```
configure network ipv6 router [management_interface]
```

Exemple :

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.
```

```
>
```

- Configuration manuelle :

```
configure network ipv6 manual ip6_address ip6_prefix_length [ip6_gateway_ip]
[management_interface]
```

Notez que *ip6_gateway_ip* dans cette commande est utilisé pour créer la voie de routage par défaut pour le périphérique. Si vous configurez une interface d'événements uniquement, vous devez entrer *ip6_gateway_ip* dans la commande; cependant, cette entrée configure simplement la voie de routage par défaut à la valeur que vous spécifiez et ne crée pas de voie de routage statique distincte pour

l'interface d'événement. Si vous utilisez une interface d'événements uniquement sur un réseau différent de l'interface de gestion, nous vous recommandons de définir *ipv6_gateway_ip* pour une utilisation avec l'interface de gestion, puis de créer une voie de routage statique séparément pour l'interface d'événements uniquement en utilisant la commande **configure network static-routes**.

Exemple :

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6 (pris en charge sur l'interface de gestion par défaut uniquement) :

configure network ipv6 dhcp

Étape 5

Pour IPv6, activez ou désactivez les réponses Echo ICMPv6 et les messages Destination Unreachable. Ceux-ci sont activés par défaut.

configure network ipv6 destination-unreachable {enable | disable}

configure network ipv6 echo-reply {enable | disable}

Vous pouvez désactiver ces paquets pour vous protéger contre d'éventuelles attaques par déni de service. La désactivation des paquets de réponse Echo signifie que vous ne pouvez pas utiliser le ping IPv6 vers les interfaces de gestion des périphériques à des fins de test.

Exemple :

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

Étape 6

Activez un serveur DHCP sur l'interface de gestion par défaut pour fournir les adresses IP aux hôtes connectés :

configure network ipv4 dhcp-server-enable start_ip_address end_ip_address

Exemple :

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

Vous pouvez uniquement configurer un serveur DHCP lorsque vous définissez l'adresse IP de l'interface de gestion manuellement. Cette commande n'est pas prise en charge sur le centre de gestion virtuel . Pour afficher l'état du serveur DHCP, saisissez **show network-dhcp-server**:

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

Étape 7

Ajouter une voie de routage statique pour l'interface d'événements uniquement si centre de gestion se trouve sur un réseau distant; sinon, tout le trafic correspondra à la voie de routage par défaut dans l'interface de gestion.

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

Pour la voie de routage *par défaut*, n'utilisez pas cette commande; vous ne pouvez modifier l'adresse IP de la passerelle de routage par défaut que lorsque vous utilisez les commandes **configure network ipv4** ou **ipv6** (voir [Étape 4](#), à la page 36).

Exemple :

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully
```

```
> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully
```

```
>
```

Pour afficher les routes statiques, saisissez **show network-static-routes** (la route par défaut n'est pas affichée) :

```
> show network-static-routes
-----[ IPv4 Static Routes ]-----
Interface           : management1
Destination         : 192.168.6.0
Gateway             : 10.10.10.1
Netmask             : 255.255.255.0
[...]
```

Étape 8

Définir le nom de domaine :

configure network hostname *nom*

Exemple :

```
> configure network hostname farscape1.cisco.com
```

Les messages syslog ne reflètent un nouveau nom d'hôte qu'après un redémarrage.

Étape 9

Définissez les domaines de recherche :

configure network dns searchdomains *domain_list*

Exemple :

```
> configure network dns searchdomains example.com,cisco.com
```

Définissez le ou les domaines de recherche pour le périphérique, séparés par des virgules. Ces domaines sont ajoutés aux noms d'hôte lorsque vous ne spécifiez pas de nom de domaine complet dans une commande, par exemple **ping system**. Les domaines sont utilisés uniquement sur l'interface de gestion ou pour les commandes qui passent par l'interface de gestion.

Étape 10

Configurez jusqu'à 3 serveurs DNS, séparés par des virgules :

configure network dns servers *dns_ip_list*

Exemple :

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

Étape 11

Définissez le port de gestion à distance pour la communication avec centre de gestion :

```
configure network management-interface tcpport nombre
```

Exemple :

```
> configure network management-interface tcpport 8555
```

Le centre de gestion et les périphériques gérés communiquent en utilisant un canal de communication bidirectionnel chiffré TLS-1.3, qui se trouve par défaut sur le port 8305.

Remarque Cisco vous recommande **fortement** de conserver les paramètres par défaut pour le port de gestion à distance, mais si le port de gestion entre en conflit avec d'autres communications de votre réseau, vous pouvez choisir un port différent. Si vous modifiez le port de gestion, vous devez le modifier pour **tous** les périphériques de votre déploiement qui doivent communiquer entre eux.

Étape 12

(Défense contre les menaces uniquement) Définissez la MTU de l'interface de gestion ou d'événement. Par défaut, la MTU est de 1500 octets.

```
configure network mtu [bytes] [interface_id]
```

- *octets* : définit la MTU en octets. Pour l'interface de gestion, la valeur peut être comprise entre 64 et 1500 si vous activez IPv4, et entre 1280 et 1500 si vous activez IPv6. Pour l'interface d'événement, la valeur peut être comprise entre 64 et 9 000 si vous activez IPv4, et entre 1 280 et 9 000 si vous activez IPv6. Si vous activez IPv4 et IPv6, le minimum est de 1 280. Si vous n'saisissez pas les *octets*, vous êtes invité à saisir une valeur.
- *interface_id* : spécifie l'ID de l'interface pour laquelle définir la MTU. Utilisez la commande **show network** pour afficher les ID d'interface disponibles, par exemple management0, management1, br1 et eth0, selon la plateforme. Si vous ne spécifiez pas d'interface, l'interface de gestion est utilisée.

Exemple :

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

Étape 13

Configurez un serveur mandataire HTTP. Le périphérique est configuré pour se connecter directement à Internet sur les ports TCP/443 (HTTPS) et TCP/80 (HTTP). Vous pouvez utiliser un serveur mandataire, auprès duquel vous pouvez vous authentifier via HTTP Digest. Après avoir exécuté la commande, vous êtes invité à saisir l'adresse et le port du mandataire HTTP, si l'authentification du mandataire est requise et, si elle est requise, le nom d'utilisateur, le mot de passe et la confirmation du mot de passe du mandataire.

Remarque Pour le mot de passe du serveur mandataire sur défense contre les menaces, vous pouvez utiliser uniquement les caractères de A à Z, a à z et de 0 à 9.

```
configure network http-proxy
```

Exemple :

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

Étape 14

Si vous modifiez l'adresse IP de gestion du périphérique, consultez les tâches suivantes pour la connectivité centre de gestion en fonction de la façon dont vous avez identifié le centre de gestion lors de la configuration initiale du périphérique à l'aide de la commande **configure manager add** :

- **Adresse IP :aucune action.** Si vous avez identifié le centre de gestion utilisant une adresse IP accessible, la connexion de gestion sera rétablie automatiquement après plusieurs minutes. Nous vous recommandons de modifier également l'adresse IP du périphérique indiquée dans centre de gestion pour maintenir la synchronisation des informations. voir [Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 15](#). Cette action peut aider la connexion à se rétablir plus rapidement. **Remarque** : si vous avez spécifié une adresse IP centre de gestion inaccessible, vous devez rétablir manuellement la connexion à l'aide de [Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 15](#).
- **ID NAT uniquement : rétablissez manuellement la connexion.** Si vous avez identifié centre de gestion en utilisant uniquement l'ID NAT, la connexion ne peut pas être rétablie automatiquement. Dans ce cas, modifiez l'adresse IP de gestion du périphérique dans centre de gestion en fonction de [Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 15](#).

Modifier l'interface de données Défense contre les menaces utilisée pour la gestion au niveau de l'interface de ligne de commande

Si la connexion de gestion entre défense contre les menaces et centre de gestion a été interrompue et que vous souhaitez spécifier une nouvelle interface de données pour remplacer l'ancienne interface, utilisez l'interface de ligne de commande défense contre les menaces pour configurer la nouvelle interface. Cette procédure suppose que vous souhaitez remplacer l'ancienne interface par une nouvelle interface sur le même réseau. Si la connexion de gestion est active, vous devez apporter des modifications à une interface de données existante à l'aide de centre de gestion. Pour la configuration initiale de l'interface de gestion des données, consultez la commande **configure network management-data-interface**.



Remarque

Cette rubrique s'applique à l'interface de données que vous avez configurée pour la gestion, et non à l'interface de gestion dédiée. Si vous souhaitez modifier les paramètres réseau pour l'interface de gestion, consultez [Modifier les interfaces de gestion Défense contre les menaces au niveau de l'interface de ligne de commande, à la page 34](#).

Pour obtenir des informations détaillées sur l'interface de ligne de commande de défense contre les menaces, consultez [Référence des commandes de défense contre les menaces de Cisco Secure Firewall](#).

Avant de commencer

- Vous pouvez créer des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide la commande **configure user add** . Vous pouvez également configurer les utilisateurs AAA en fonction de [Authentification extérieure](#).

Procédure

Étape 1 Si vous remplacez l'interface de gestion des données par une nouvelle interface, déplacez le câble d'interface actuel vers la nouvelle interface.

Étape 2 Connectez-vous à l'interface de ligne de commande du périphérique.
Vous devez utiliser le port de console lorsque vous utilisez ces commandes. Si vous effectuez la configuration initiale, il se peut que vous soyez déconnecté de l'interface de gestion. Si vous modifiez la configuration en raison d'une connexion de gestion interrompue et que vous avez un accès SSH à l'interface de gestion dédiée, vous pouvez utiliser cette connexion SSH.

Étape 3 Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 4 Désactivez l'interface pour pouvoir reconfigurer ses paramètres.

configure network management-data-interface disable

Exemple :

```
> configure network management-data-interface disable
```

```
Configuration updated successfully..!!
```

```
Configuration disable was successful, please update the default route to point to a gateway
on management interface using the command 'configure network'
```

Étape 5 Configurez l'interface de données pour l'accès du gestionnaire.

configure network management-data-interface

Vous êtes ensuite invité à configurer les paramètres réseau de base pour l'interface de données.

Lorsque vous remplacez l'interface de gestion des données par une nouvelle interface sur le même réseau, utilisez les mêmes paramètres que pour l'interface précédente, sauf l'ID d'interface. De plus, en ce qui concerne l'option de **Do you wish to clear all the device configuration before applying ? (Souhaitez-vous effacer toute la configuration du périphérique avant de l'appliquer?) (y/n) [n] :**, choisissez **y**. (oui) Ce choix effacera l'ancienne configuration de l'interface de gestion des données, de sorte que vous puissiez réutiliser avec succès l'adresse IP et le nom d'interface sur la nouvelle interface.

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y
```

```
Configuration done with option to allow manager access from any network, if you wish to
```

```
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.
```

```
Setting IPv4 network configuration.
Network settings changed.
```

```
>
```

Étape 6 (Facultatif) Limitez l'accès aux interfaces de données à centre de gestion sur un réseau particulier.

configure network management-data-interface client *ip_address netmask*

Par défaut, tous les réseaux sont autorisés.

Étape 7 La connexion sera rétablie automatiquement, mais la désactivation et la réactivation de la connexion sur centre de gestion aideront la connexion à se rétablir plus rapidement. Consultez [Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 15](#).

Étape 8 Vérifiez que la connexion de gestion a été rétablie.

sftunnel-status-brief

Consultez l'exemple de sortie suivant au sujet d'une connexion établie avec affichage des informations sur le canal homologue et la pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
'10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Étape 9 Dans centre de gestion, choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Device(Périphériques) > Management (Gestion) > Manager Access - Configuration Details(Accès au gestionnaire - Détails de la configuration)** (FMC Access - Détails de la configuration), et cliquez sur **Refresh**(Réactualiser).

centre de gestion détecte les modifications de l'interface et de configuration de route par défaut, et bloque le déploiement sur défense contre les menaces . Lorsque vous modifiez les paramètres d'interface de données localement sur le périphérique, vous devez rapprocher ces modifications de centre de gestion manuellement. Vous pouvez afficher les écarts entre les centre de gestion et les défense contre les menaces sous l'onglet **Configuration**.

Étape 10 Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Interfaces**(interfaces) et apportez les modifications suivantes.

- Supprimez l'adresse IP et le nom de l'ancienne interface de gestion des données et désactivez l'accès du gestionnaire pour cette interface.
- Configurez la nouvelle interface de gestion des données avec les paramètres de l'ancienne interface (celles que vous utilisiez au niveau de l'interface de ligne de commande) et activez l'accès de gestionnaire pour celle-ci.

Étape 11 Choisissez **Devices (Périphériques) > Device Management(Gestion des périphériques) > Routing (Routage) > Static Route (Routage statique)** et modifiez le routage par défaut de l'ancienne interface de gestion de données à la nouvelle.

Étape 12

Revenez à la boîte de dialogue **Manager Access – Configuration Details**(Accès au gestionnaire - Détails de la configuration) (FMC Access - Détails de la configuration), puis cliquez sur **Acknowledge** (Accusé de réception) pour supprimer le blocage de déploiement.

Lors du prochain déploiement, la configuration centre de gestion remplacera tous les paramètres en conflit restants sur défense contre les menaces . Il est de votre responsabilité de corriger manuellement la configuration centre de gestion avant de procéder au redéploiement.

Vous verrez les messages attendus « La configuration a été effacée » et « L'accès du gestionnaire a été modifié et confirmé par un accusé de réception ».

Restaurer manuellement la configuration si le Centre de gestion perd la connexion

Si vous utilisez une interface de données sur le défense contre les menaces pour l'accès du gestionnaire, et que vous déployez un changement de configuration du centre de gestion qui a des répercussions sur la connectivité du réseau, vous pouvez restaurer la configuration sur le défense contre les menaces à la dernière configuration déployée afin de pouvoir restaurer la connexion de gestion. Vous pouvez ensuite ajuster les paramètres de configuration dans centre de gestion de manière à maintenir la connexion au réseau, et redéployer. Vous pouvez utiliser la fonction de restauration même si vous ne perdez pas la connectivité. Cela ne se limite pas à ce dépannage.

Vous pouvez également activer la restauration automatique de la configuration si vous perdez la connectivité après un déploiement; voir [Modifier les paramètres de déploiement, à la page 61](#).

Consultez les consignes suivantes :

- Seul le déploiement précédent est disponible localement sur défense contre les menaces ; vous ne pouvez pas restaurer les déploiements précédents.
- La restauration est prise en charge pour la haute disponibilité mais pas pour les déploiements de mise en grappe.
- La restauration n'est pas prise en charge immédiatement après la création de la haute disponibilité.
- Le restaurer ne vise que les configurations que vous pouvez définir dans l'application centre de gestion. Par exemple, la restauration ne touche aucune configuration locale liée à l'interface de commande dédiée, que vous ne pouvez configurer qu'au niveau de l'interface de ligne de commande défense contre les menaces . Notez que si vous avez modifié les paramètres de l'interface de données après le dernier centre de gestion déploiement à l'aide de la commande **configure network management-data-interface**, et que vous utilisez ensuite la commande de restauration, ces paramètres ne seront pas conservés ; ils seront restaurés aux paramètres centre de gestion déployés en dernier lieu.
- Le mode UCAPL/CC ne peut pas être annulé.
- Les données de certificat SCEP hors bande qui ont été mises à jour lors du déploiement précédent ne peuvent pas être restaurées.
- Pendant la restauration, les connexions seront interrompues, car la configuration actuelle sera effacée.

Procédure

Étape 1

À l'interface de ligne de commande défense contre les menaces , restaurez la configuration précédente.

configure policy rollback

Remarque Pour une paire à haute disponibilité, cette commande n'est autorisée que sur l'unité active.

Après la restauration, le défense contre les menaces notifie le centre de gestion que la restauration a été effectuée avec succès. Dans le centre de gestion, l'écran de déploiement affiche une enseigne indiquant que la configuration a été restaurée.

Remarque Si la restauration échoue et que le gestionnaire centre de gestion est restauré, reportez-vous à <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html> pour connaître les problèmes de déploiement courants. Dans certains cas, la restauration peut échouer après le rétablissement de l'accès au gestionnaire centre de gestion; dans ce cas, vous pouvez résoudre les enjeux de configuration centre de gestion et redéployer à partir du centre de gestion.

Exemple :

Pour le défense contre les menaces qui utilise une interface de données pour l'accès du gestionnaire :

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....
.....
>
```

Exemple :

Pour les défense contre les menaces d'une paire à haute disponibilité qui utilisent une interface de données pour l'accès centre de gestion :

```
> configure policy rollback

Checking Eligibility ....
===== DEVICE DETAILS =====
Device Version: 7.2.0
Device Type: FTD
Device Mode: Offbox
Device in HA: true
Is HA disabled: false
HA state: active - standby ready
=====
Device is eligible for policy rollback
Do you want to continue [YES/NO]?

YES

Starting rollback...
  Preparing policy configuration on the device.           Status: success
  Applying updated policy configuration on the device.    Status: success
  Applying Lina File Configuration on the device.        Status: success
  Applying Lina Configuration on the device.             Status: success
```

```

Commit Lina Configuration.                Status: success
Commit Lina File Configuration.           Status: success
Commit Lina File Configuration.           Status: success
=====
POLICY ROLLBACK STATUS: SUCCESS
=====
>

```

Étape 2 Vérifiez que la connexion de gestion a été rétablie.

Dans centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils) > Device Management (gestion de l'appareil) > Device (appareil) > Management (gestion) > Manager Access - Configuration Details (accès du gestionnaire - Détails de la configuration) > Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez [Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 45](#).

Résoudre les problèmes de connectivité de gestion sur l'interface de données

Lorsque vous utilisez une interface de données pour l'accès du gestionnaire au lieu d'utiliser l'interface de gestion dédiée, vous devez faire attention à ne pas modifier les paramètres d'interface et de réseau du défense contre les menaces dans le centre de gestion pour ne pas interrompre la connexion. Si vous changez le type d'interface de gestion après avoir ajouté le défense contre les menaces au centre de gestion (de données à gestion, ou de gestion à données), si les interfaces et les paramètres réseau ne sont pas configurés correctement, vous pouvez perdre la connectivité de gestion.

Cette rubrique vous aide à résoudre les problèmes de perte de connectivité de gestion.

Afficher l'état de la connexion de gestion

Dans le centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils) > Device Management (gestion de l'appareil) > Device (appareil) > Management (gestion) > Manager Access - Configuration Details (accès du gestionnaire - Détails de la configuration) > Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion. Vous pouvez également utiliser la commande **sftunnel-status** pour afficher des informations plus complètes.

Consultez l'exemple de sortie suivant au sujet d'une connexion interrompue; il n'y a pas d'information de connexion à un canal homologue, ni aucune information de pulsation :

```

> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down

```

Consultez l'exemple de sortie suivant au sujet d'une connexion établie avec affichage des informations sur le canal homologue et la pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Voir les informations sur le réseau défense contre les menaces

Dans l'interface de la ligne de commande défense contre les menaces, affichez les paramètres de réseau de l'interface de données de gestion et d'accès du gestionnaire :

show network

```
> show network
===== [ System Information ] =====
Hostname                : FTD-4
Domains                 : cisco.com
DNS Servers             : 72.163.47.11
DNS from router        : enabled
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces

===== [ management0 ] =====
Admin State             : enabled
Admin Speed             : 1gbps
Operation Speed        : 1gbps
Link                   : up
Channels                : Management & Events
Mode                   : Non-Autonegotiation
MDI/MDIX               : Auto/MDIX
MTU                    : 1500
MAC Address            : 68:87:C6:A6:54:80
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 10.89.5.4
Netmask                : 255.255.255.192
Gateway                : 169.254.1.1
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                  : Disabled
Authentication         : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers            : 72.163.47.11
Interfaces             : Ethernet1/1

===== [ Ethernet1/1 ] =====
State                  : Enabled
Link                   : Up
Name                   : outside
MTU                    : 1500
MAC Address            : 68:87:C6:A6:54:A4
----- [ IPv4 ] -----
Configuration          : Manual
```

```

Address                : 10.89.5.6
Netmask                : 255.255.255.192
Gateway                : 10.89.5.1
-----[ IPv6 ]-----
Configuration          : Disabled

```

Vérifiez que défense contre les menaces est enregistré auprès du centre de gestion

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que l'enregistrement centre de gestion a été effectué. Remarque : Cette commande n'affichera pas l'état *actuel* de la connexion de gestion.

show managers

```

> show managers
Type                : Manager
Host                : 10.10.1.4
Display name        : 10.10.1.4
Identifiant         : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration        : Completed
Management type     : Configuration

```

Envoyez un message Ping au centre de gestion

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer une commande d'envoi de message Ping à centre de gestion à partir des interfaces de données :

ping *fmc_ip*

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer un message Ping à centre de gestion à partir de l'interface de gestion, qui devrait être distribuée par le fond de panier vers les interfaces de données :

ping system *fmc_ip*

Saisissez les paquets sur l'interface interne défense contre les menaces

Dans l'interface de ligne de commande défense contre les menaces , saisissez les paquets sur l'interface interne du fond de panier (*nlp_int_tap*) pour voir si des paquets de gestion sont envoyés :

capture *nom* interface *nlp_int_tap* trace detail match ip any any

show capture *nom* trace detail

Vérifier l'état de l'interface interne, les statistiques et le nombre de paquets

Dans l'interface de ligne de commande défense contre les menaces , voir les informations sur l'interface interne du fond de panier, *nlp_int_tap* :

show interface detail

```

> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
  (Full-duplex), (1000 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0000.0100.0001, MTU 1500
  IP address 169.254.1.1, subnet mask 255.255.255.248
  37 packets input, 2822 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants

```

```

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
5 packets output, 370 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
37 packets input, 2304 bytes
5 packets output, 300 bytes
37 packets dropped
  1 minute input rate 0 pkts/sec,  0 bytes/sec
  1 minute output rate 0 pkts/sec,  0 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec,  0 bytes/sec
  5 minute output rate 0 pkts/sec,  0 bytes/sec
  5 minute drop rate, 0 pkts/sec
Control Point Interface States:
Interface number is 14
Interface config status is active
Interface state is active

```

Vérifiez le routage et la NAT

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que la route par défaut (S*) a été ajoutée et que des règles NAT internes existent pour l'interface de gestion (nlp_int_tap).

show route

```

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C       10.89.5.0 255.255.255.192 is directly connected, outside
L       10.89.5.29 255.255.255.255 is directly connected, outside

>

```

show nat

```

> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface service
  tcp 8305 8305
  translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
  tcp ssh ssh

```



```

    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6 service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>

```

Vérifier les autres paramètres

Consultez les commandes suivantes pour vérifier que tous les autres paramètres sont présents. Vous pouvez également voir plusieurs de ces commandes sur la page de centre de gestion **Devices (appareils) > Device Management > Device (appareil) > Management (gestion) > Manager Access - Configuration Details (accès du gestionnaire - Détails de la configuration) > CLI Output (extrait de l'interface de ligne de commande)**.

show running-config sftunnel

```

> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305

```

show running-config ip-client

```

> show running-config ip-client
ip-client outside

```

show conn address *fmc_ip*

```

> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
    preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
bytes 1630834, flags UIO
>

```

Faire une recherche de mise à jour DDNS réussie

Dans l'interface de ligne de commande défense contre les menaces, vérifiez si la mise à niveau DDNS a réussi :

debug ddns

```

> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0

```

Si la mise à jour échoue, utilisez les commandes **debug http** et **debug ssl**. Pour les échecs de validation de certificat, vérifiez que les certificats racine sont installés sur le périphérique comme suit :

show crypto ca certificates *trustpoint_name*

Pour vérifier le fonctionnement du DDNS :

```
show ddns update interface fmc_access_ifc_name
```

```
> show ddns update interface outside
```

```
Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available
```

```
Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Vérifier les fichiers journaux centre de gestion

See <https://cisco.com/go/fmc-reg-error>.

Résoudre les problèmes de connectivité de gestion sur l'interface de données sur une paire à haute disponibilité

Cette rubrique vous aide à résoudre la perte de connectivité de gestion sur une interface de données en haute disponibilité.

Prise en charge des modèles—Défense contre les menaces

La connexion de gestion entre l'homologue actif et CDO peut être interrompue pour les raisons suivantes :

- L'interface de données utilisée pour la gestion sur l'unité active présente des problèmes de connectivité.

Vous devez basculer manuellement vers l'unité de secours, puis configurer une nouvelle interface de données pour l'accès à CDO.

- Le fournisseur d'accès à Internet a changé.

Vous devez mettre à jour manuellement les nouveaux détails du réseau sur l'unité active à l'aide des commandes CLI pour restaurer la connectivité du périphérique avec CDO.

L'interface de gestion des données sur l'unité active présente des problèmes de connectivité

1. Dans CDO, mettez manuellement l'unité active en veille. Consultez [Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces](#).

Sinon, vous pouvez exécuter la commande **no failover active** sur l'unité active.

Le périphérique en veille devient le nouveau périphérique actif dans la paire à haute disponibilité et établit la communication avec CDO.

2. À côté de la paire de périphériques à haute disponibilité que vous souhaitez modifier, cliquez sur **Modifier** (✎).
3. Choisissez **Routage > Route statique** et supprimez la voie de routage statique définie pour l'ancienne interface de gestion des données.
4. Cliquez sur l'onglet **Interfaces** et apportez les modifications suivantes.
 1. Supprimez l'adresse IP et le nom de l'ancienne interface de gestion des données et désactivez l'accès à CDO pour cette interface.

**Remarque**

Avant de supprimer les anciennes informations de l'interface de gestion des données, souvenez-vous des détails si vous souhaitez utiliser les mêmes informations.

1. Cliquez sur **Modifier** (✎) à côté de l'interface que vous souhaitez supprimer.

The screenshot shows the 'Edit Physical Interface' configuration window. At the top, there are tabs for 'General', 'IPv4', 'IPv6', 'Advanced', 'Path Monitoring', and 'Hardware Configuration'. Below the tabs, there is a section for 'Firewall Management Center Access'. The 'Name' field is set to 'outside'. The 'Enabled' checkbox is checked, and the 'Management Only' checkbox is unchecked. The 'Description' field is empty.

2. Effacez le contenu du champ **Nom**.
 3. Décochez la case **Activé**.
 4. Dans l'onglet **IPv4** ou **IPv6**, supprimez l'adresse active.
 5. Dans l'onglet **Accès au centre de gestion Cisco Firewall Management Center**, décochez **Activer la gestion sur cette interface pour le centre de gestion Cisco Firepower Management Center**.
 6. Cliquez sur **OK**.
 7. Cliquez sur **Yes** (oui) pour confirmer les modifications.
2. Configurez la nouvelle interface de gestion des données avec les paramètres de l'ancienne interface (celles que vous utilisiez au niveau de l'interface de ligne de commande) et activez l'accès CDO pour celle-ci.
 1. Cliquez sur **Edit** (Modifier) (✎) à côté de l'interface de données que vous souhaitez utiliser pour gérer le trafic de gestion.
 2. Dans le champ **Name**, spécifiez un nom pour l'interface.
 3. Cochez la case **Activé**.
 4. Dans l'onglet **IPv4** ou **IPv6**, spécifiez l'adresse active.
 5. Dans l'onglet **Accès au centre de gestion Cisco Firewall Management Center**, cochez **Activer la gestion sur cette interface pour le centre de gestion Cisco Firepower Management Center**.
 6. Cliquez sur **OK**.
 7. Cliquez sur **Yes** (oui) pour confirmer les modifications.

5. Cliquez sur l'onglet **High Availability** (haute disponibilité) et apportez les modifications suivantes.
 1. Dans la zone **Monitored Interfaces** (interfaces surveillées), cliquez sur le bouton **Edit** (Modifier) (✎) à côté de la nouvelle interface de gestion des données.

Monitored Interfaces						
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitor
outside-new	192.168.0.11					
diagnostic						

Active IP Address (adresse IP active) indique l'adresse IP du périphérique actif.

2. Dans l'onglet **IPv4**, saisissez l'**adresse IP de secours** et l'adresse de la **passerelle**.

Edit outside-new ?

Monitor this interface for failures

IPv4 IPv6

Interface Name:
outside-new

Active IP Address:
192.168.0.11

Mask:
255.255.255.0

Standby IP Address:

3. Si vous avez configuré l'adresse IPv6 manuellement, dans l'onglet IPv6, cliquez sur **Edit** (Modifier) (✎) à côté de l'adresse IP active, saisissez l'**adresse IP de secours**, puis cliquez sur **OK**.
4. Cliquez sur **OK**.
6. Cliquez sur **Save** (Enregistrer) dans le coin supérieur droit pour enregistrer les modifications.
7. Choisissez **Routage > Route statique** et ajoutez la voie de routage statique définie pour la nouvelle interface de gestion des données. La nouvelle interface de données apparaît dans la liste **Interface**.

Add Static Route Configuration ?

Type: IPv4 IPv6

Interface*

Null0 if it is available for route leak

outside-new (Firewall Management Center Access) Selected Network

diagnostic

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Gateway* +

8. Cliquez sur **Save** (Enregistrer) dans le coin supérieur droit pour enregistrer les modifications.
9. Déployer les changements de configuration..
10. Lorsque le déploiement est terminé à environ 90 %, la nouvelle interface de gestion prend effet. À ce stade, vous devez rebrancher le FTD de sorte que CDO atteigne le FTD sur la nouvelle interface et termine le déploiement avec succès.



Remarque

Après le re-câblage, le déploiement peut échouer s'il a expiré avant de rétablir la connexion de gestion à la nouvelle interface. Dans ce cas, vous devez relancer le déploiement après le recâblage pour un déploiement réussi.

11. Vérifiez que la connexion de gestion a été rétablie.

Dans Centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils) > Device Management (gestion des appareils) > Device (appareil) > Management (gestion) > FMC Access Details (détails de l'accès FMC) > Connection Status (état de la connexion)**.

Sinon, au niveau de l'interface de ligne de commande FTD, entrez la commande `sftunnel-status-brief` pour afficher l'état de la connexion de gestion.

Le fournisseur d'accès à Internet a changé.

Si vous avez changé de fournisseur de services Internet, vous pouvez perdre la connectivité de gestion, même si l'intégrité de la haute disponibilité est normale. Configurez les nouveaux détails réseau de l'interface de gestion à l'aide des commandes de l'interface de ligne de commande.



Remarque

Ces commandes sont disponibles uniquement sur l'unité active et non en veille.

Pour des informations sur l'interface de ligne de commande défense contre les menaces, voir la [référence des commandes FTD](#).

1. Connectez-vous à l'interface de ligne de commande du périphérique.

Vous devez utiliser le port de console lorsque vous utilisez ces commandes. Si vous modifiez la configuration en raison d'une connexion de gestion interrompue et que vous avez un accès SSH à l'interface de gestion dédiée, vous pouvez utiliser cette connexion SSH.

Consultez [Connexion à l'interface de ligne de commande \(CLI\) sur le périphérique](#).

2. Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.
3. Utilisez l'une des commandes suivantes selon la valeur réseau que vous souhaitez mettre à jour :

- **configure network management-data-interface ipv4 manual** *ip_address ip_netmask interface interface_id*
- **configure network management-data-interface ipv4 gateway_ip** *interface interface_id*
- **configure network management-data-interface ipv4 manual** *ip_address ipv4_netmask gateway_ip interface interface_id*

Exemple :

```
Configure network management-data-interface ipv4 manual 10.10.6.7 255.255.255.0 interface
gig0/0
Configuration updated successfully.!!!
```



Remarque Toutes les autres commandes CLI de **configure network management-data-interface** ne sont pas prises en charge sur les périphériques dans une paire à haute disponibilité.

La configuration est automatiquement envoyée au périphérique en veille.

4. **Facultatif** Limitez l'accès aux interfaces de données à CDO sur un réseau particulier.

configure network management-data-interface client *ip_address netmask*

Par défaut, tous les réseaux sont autorisés.

5. Vérifiez que la connexion de gestion a été rétablie.

sftunnel-status-brief

Consultez l'exemple de sortie suivant au sujet d'une connexion établie avec affichage des informations sur le canal homologue et la pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

6. Dans CDO, cliquez sur **Inventory** (Inventaire) > **FTD**.

7. Sélectionnez votre défense contre les menaces et dans le volet **Management** (Gestion) à droite, cliquez sur **Device Summary** (Résumé du périphérique).

8. Dans **Management > FMC Access Details**(Gestion > détails de l'accès à FMC), cliquez sur **Refresh**(actualiser).

CDO détecte les modifications de l'interface et de la configuration de la route par défaut, et bloque le déploiement sur FTD. Lorsque vous modifiez les paramètres d'interface de données localement sur le périphérique, vous devez rapprocher ces modifications dans CDO manuellement. Vous pouvez afficher les écarts entre CDO et défense contre les menaces sous l'onglet **Configuration**.

9. Revenez à la boîte de dialogue **FMC Access Details** (détails de l'accès FMC), et cliquez sur **Acknowledge** (accusé de réception) pour supprimer le blocage de déploiement.

Lors du prochain déploiement, la configuration CDO remplacera tous les paramètres en conflit restants sur FTD. Il est de votre responsabilité de corriger manuellement la configuration CDO avant de procéder au redéploiement.


Vous verrez les messages attendus « La configuration a été effacée » et « Accès FMC modifié et confirmé. »

La modification de configuration effectuée sur l'unité active est automatiquement mise en veille. Une fois que CDO a rétabli sa connectivité avec l'unité active, CDO met à jour l'adresse IP de secours.

Afficher les détails de l'inventaire

La section **Inventory Details** de la page **Device** affiche les détails du châssis tels que le processeur et la mémoire.

Illustration 29 : Détails de l'inventaire

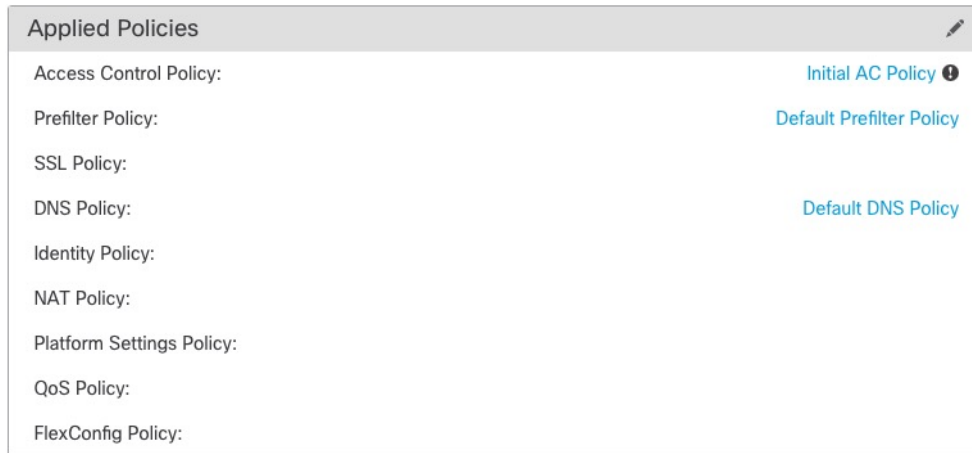
Inventory Details 	
CPU Type:	CPU Xeon E5 series 2300 MHz
CPU Cores:	1 CPU (4 cores)
Memory:	8192 MB RAM
Storage:	N/A
Chassis URL:	N/A
Chassis Serial Number:	N/A
Chassis Module Number:	N/A
Chassis Module Serial Number:	N/A

Pour mettre à jour les renseignements, cliquez sur **Actualisation** .

Modifier les politiques appliquées

La section **Politiques appliquées** de la page **Périphérique** affiche les politiques suivantes appliquées à votre pare-feu :

Illustration 30 : Politiques appliquées



Pour les politiques avec des liens, vous pouvez cliquer sur le lien pour afficher la politique.

Pour la politique de contrôle d'accès, affichez la boîte de dialogue **Informations sur la politique d'accès pour le dépannage** en cliquant sur l'icône **Exclamation** ⓘ. Cette boîte de dialogue montre comment les règles d'accès sont développées en entrées de contrôle d'accès (ACE).

Illustration 31 : Information sur la stratégie d'accès pour le dépannage



Vous pouvez affecter des politiques à un périphérique individuel à partir de la page **Device Management** (gestion des périphériques).

Procédure

- Étape 1** Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.
- Étape 2** En regard du périphérique auquel vous souhaitez affecter des politiques, cliquez sur **Edit** (✎).
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.
- Étape 3** Cliquez sur **Device (périphérique)**.
- Étape 4** Dans la section **Politiques appliquées**, cliquez sur **Edit** (✎).

Illustration 32 : Attributions de stratégie

Policy Assignments ?

Access Control Policy: Initial AC Policy

NAT Policy: None

Platform Settings Policy: None

QoS Policy: None

FlexConfig Policy: None

Cancel Save

- Étape 5** Pour chaque type de politique, choisissez une politique dans le menu déroulant. Seules les politiques existantes sont répertoriées.
- Étape 6** Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Modifier les paramètres avancés

La section **Advanced Settings** (Paramètres avancés) de la page **Device** (Périphériques) affiche un tableau des paramètres de configuration avancés, comme décrit ci-dessous. Vous pouvez modifier n'importe lequel de ces paramètres.

Tableau 5 : Champs du tableau de la section avancée

Champ	Description
Contournement de l'application	L'état du contournement automatique des applications sur le périphérique.
Seuil de contournement	Le seuil de contournement automatique des applications, en millisecondes.

Champ	Description
Recherche groupée d'objets	<p>L'état de la recherche de groupe d'objets sur le périphérique. Pendant le fonctionnement, le périphérique FTD étend les règles de contrôle d'accès en plusieurs entrées de liste de contrôle d'accès en fonction du contenu de tout réseau ou objet d'interface utilisé dans la règle d'accès. Vous pouvez réduire la mémoire requise pour rechercher des règles de contrôle d'accès en activant la recherche par groupe d'objets. Lorsque la recherche par groupe d'objets est activée, le système ne développe pas les objets d'interface ou de réseau, mais recherche plutôt les règles d'accès pour les correspondances en fonction des définitions de ces groupes. La recherche par groupe d'objets n'a aucune incidence sur la façon dont vos règles d'accès sont définies ou sur la façon dont elles s'affichent dans le centre de gestion Cisco Firepower Management Center. Il a une incidence uniquement sur la façon dont le périphérique les interprète et les traite lors de la mise en correspondance des connexions avec les règles de contrôle d'accès.</p> <p>Remarque Par défaut, la recherche de groupe d'objets est activée lorsque vous ajoutez la solution de défense contre les menaces pour la première fois dans le centre de gestion.</p>
Objet d'optimisation de l'interface	<p>L'état de l'optimisation des objets d'interface sur le périphérique. Pendant le déploiement, les groupes d'interfaces et les zones de sécurité utilisés dans les stratégies de contrôle d'accès et de préfiltre génèrent des règles distinctes pour chaque paire d'interfaces source/de destination. Si vous activez l'optimisation des objets d'interface, le système déploiera plutôt une seule règle par contrôle d'accès ou règle de préfiltre, ce qui peut simplifier la configuration de l'appareil, utiliser moins de mémoire système et améliorer la performance du déploiement. Si vous sélectionnez cette option, sélectionnez également l'option Object Group Search (Recherche de groupe d'objets) pour réduire l'utilisation de la mémoire du périphérique.</p>

Les rubriques suivantes expliquent comment modifier les paramètres avancés du périphérique.



Remarque Pour en savoir plus sur le paramètre Transférer les paquets, consultez [Modifier les paramètres généraux](#), à la page 6.

Configurer le contournement automatique de l'application

Le contournement automatique des applications (AAB) permet aux paquets de contourner la détection si Snort est en panne ou, pour un périphérique classique, si un paquet prend trop de temps à traiter. La fonction AAB entraîne le redémarrage Snort dans les dix minutes suivant la défaillance et génère des données de dépannage qui peuvent être analysées pour enquêter sur la cause de la défaillance Snort.



Mise en garde L'activation de la fonction AAB redémarre partiellement le processus Snort, ce qui interrompt temporairement l'inspection de quelques paquets. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez [Comportement du trafic au redémarrage de Snort](#) pour obtenir de plus amples renseignements.

Observez le comportement suivant :

Comportement FTD : si Snort est en panne, l'AAB est déclenché après la durée spécifiée de la minuterie. Si Snort est activé, la fonction AAB n'est jamais déclenchée, même si le traitement des paquets dépasse la minuterie configurée.

Comportement de périphérique classique : la fonctionnalité AAB limite le temps alloué pour traiter les paquets via une interface. Vous équilibrez les retards de traitement des paquets avec la tolérance de votre réseau pour la latence des paquets.

La fonctionnalité fonctionne avec n'importe quel déploiement; cependant, elle est plus utile dans les déploiements en ligne.

En règle générale, vous utilisez la règle de seuil de latence dans la politique de prévention des intrusions pour accélérer les paquets une fois que la valeur de seuil de latence est dépassée. La règle de seuil de latence n'arrête pas le moteur et ne génère pas de données de dépannage.

Si la détection est contournée, le périphérique génère une alerte de surveillance de l'intégrité.

Par défaut, l'AAB est désactivé; Pour activer le protocole AAB, suivez les étapes décrites.

Procédure

-
- Étape 1** Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.
- Étape 2** En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** (✎).
- Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.
- Étape 3** Cliquez sur **Périphériques**, puis sur **Edit** (✎) dans la section des **paramètres avancés**.
- Étape 4** Cochez **Contournement automatique de l'application**.
- Étape 5** Saisissez un **seuil de contournement** compris entre 250 ms et 60 000 ms. La valeur par défaut est de 3 000 millisecondes (ms).
- Étape 6** Cliquez sur **Save** (enregistrer).
-

Prochaine étape

- Déployer les changements de configuration.

Configurer la recherche groupée d'objets

Pendant son fonctionnement, le périphérique défend contre les menaces étend les règles de contrôle d'accès en plusieurs entrées de liste de contrôle d'accès en fonction du contenu de tout objet de réseau ou d'interface utilisé dans la règle d'accès. Vous pouvez réduire la mémoire requise pour rechercher des règles de contrôle d'accès en activant la recherche par groupe d'objets. Lorsque la recherche par groupe d'objets est activée, le système ne développe pas les objets d'interface ou de réseau, mais recherche plutôt les règles d'accès pour les correspondances en fonction des définitions de ces groupes. La recherche par groupe d'objets n'a aucune incidence sur la façon dont vos règles d'accès sont définies ou sur la façon dont elles s'affichent dans centre de gestion. Il a une incidence uniquement sur la façon dont le périphérique les interprète et les traite lors de la mise en correspondance des connexions avec les règles de contrôle d'accès.

L'activation de la recherche de groupe d'objets réduit les besoins en mémoire pour les politiques de contrôle d'accès qui incluent des objets réseau ou d'interface. Cependant, il est important de noter que la recherche par groupe d'objets peut également diminuer les performances de la recherche de règles et donc augmenter l'utilisation de l'unité centrale. Vous devez équilibrer l'incidence sur le processeur et le besoin en mémoire réduits pour la stratégie de contrôle d'accès spécifique. Dans la plupart des cas, l'activation de la recherche de groupe d'objets offre une nette amélioration opérationnelle.

par défaut, la recherche de groupe d'objets est activée pour les périphériques de défense contre les menaces qui sont ajoutés pour la première fois dans centre de gestion. Dans le cas de périphériques mis à niveau, si le périphérique est configuré avec la recherche de groupe d'objets désactivée, vous devez l'activer manuellement. Vous ne pouvez l'activer que sur un périphérique à la fois; vous ne pouvez pas l'activer globalement. Nous vous recommandons de l'activer sur tout périphérique sur lequel vous déployez des règles d'accès qui utilisent des objets réseau ou d'interface .



Remarque

Si vous activez la recherche de groupe d'objets, puis configurez et utilisez le périphérique pendant un certain temps, sachez que la désactivation de la fonction par la suite pourrait entraîner des résultats indésirables. Si vous désactivez la recherche de groupe d'objets, vos règles de contrôle d'accès existantes seront développées dans la configuration du périphérique en cours d'exécution. Si l'expansion exige plus de mémoire qu'il en est disponible, votre appareil pourrait se trouver dans un état incohérent et cela pourrait causer un impact sur la performance. Si votre périphérique fonctionne normalement, vous ne devez pas désactiver la recherche de groupe d'objets une fois que vous l'avez activée.

Avant de commencer

- Prise en charge des modèles—Défense contre les menaces
- Nous vous recommandons d'activer également la validation transactionnelle sur chaque périphérique. Dans la console de l'interface de ligne de commande, saisissez la commande **asp rule-engine transactional-commit access-group**.
- La modification de ce paramètre peut perturber le fonctionnement du système pendant que le périphérique recompile les listes de contrôle d'accès. Nous vous recommandons de modifier ce paramètre au cours d'une fenêtre de maintenance.

Procédure

- Étape 1** Choisissez **Devices (périphériques) > Device Management (gestion des périphériques)**.
- Étape 2** À côté du périphérique défense contre les menaces sur lequel vous souhaitez configurer la règle, cliquez sur le bouton **Edit** (✎).
- Étape 3** Cliquez sur l'onglet **Device** (périphérique), puis sur **Edit** (✎) dans la section **Advanced Settings** (paramètres avancés).
- Étape 4** Cochez **(Object Group Search** (Recherche par groupe d'objets).
- Étape 5** Pour que la recherche par groupe d'objets fonctionne sur les objets d'interface en plus des objets réseau, consultez **Optimisation des objets d'interface**.

Si vous ne sélectionnez pas **Optimisation des objets d'interface**, le système déploie des règles distinctes pour chaque paire source/interface, au lieu d'utiliser les zones de sécurité et les groupes d'interfaces utilisés

dans les règles. Cela signifie que les groupes d'interface ne sont pas disponibles pour le traitement de recherche de groupes d'objets.

Étape 6 Cliquez sur **Save** (enregistrer).

Configurer l'optimisation des objets d'interface

Pendant le déploiement, les groupes d'interfaces et les zones de sécurité utilisés dans les stratégies de contrôle d'accès et de préfiltre génèrent des règles distinctes pour chaque paire d'interfaces source/de destination. Si vous activez l'optimisation des objets d'interface, le système déploiera plutôt une seule règle par contrôle d'accès ou règle de préfiltre, ce qui peut simplifier la configuration de l'appareil, utiliser moins de mémoire système et améliorer la performance du déploiement. Si vous sélectionnez cette option, sélectionnez également l'option **Object Group Search** (Recherche d'objet de groupe) pour réduire l'utilisation de la mémoire du périphérique.

L'optimisation des objets d'interface est désactivée par défaut. Vous ne pouvez l'activer que sur un périphérique à la fois; vous ne pouvez pas l'activer globalement.



Remarque

Si vous désactivez l'optimisation des objets d'interface, vos règles de contrôle d'accès existantes seront déployées sans utiliser d'objets d'interface, ce qui peut prolonger le déploiement. En outre, si la recherche par groupe d'objets est activée, ses avantages ne s'appliqueront pas aux objets d'interface, et vous pourriez voir une expansion dans les règles de contrôle d'accès dans la configuration d'exécution du périphérique. Si l'expansion exige plus de mémoire qu'il en est disponible, votre appareil pourrait se trouver dans un état incohérent et cela pourrait causer un impact sur la performance.

Avant de commencer

Prise en charge des modèles—Défense contre les menaces

Procédure

- Étape 1** Choisissez **Devices (périphériques) > Device Management (gestion des périphériques)**.
- Étape 2** À côté du périphérique FTD pour lequel vous souhaitez configurer la règle, cliquez sur le bouton **Edit** (✎).
- Étape 3** Cliquez sur l'onglet **Device** (périphérique), puis sur **Edit** (✎) dans la section **Advanced Settings** (paramètres avancés).
- Étape 4** Cochez **Interface Object Optimisation** (Optimisation des objets d'interface)
- Étape 5** Cliquez sur **Save** (enregistrer).

Modifier les paramètres de déploiement

La section **Deployment Settings (paramètres de déploiement)** de la page **Device (Périphérique)** affiche les informations décrites dans le tableau ci-dessous.

Illustration 33 : Paramètres de déploiement

Deployment Settings	
Auto Rollback Deployment if Connectivity fails	Disabled
Connectivity Monitor Interval (in Minutes) ⓘ	20 Mins.

Tableau 6 : Paramètres de déploiement

Champ	Description
Déploiement avec restauration automatique si la connectivité se perd	Activé ou désactivé. Vous pouvez activer la restauration automatique si la connexion de gestion échoue à la suite du déploiement; en particulier si vous utilisez des données pour l'accès au centre de gestion, puis si vous configurez mal l'interface de données.
Intervalle de contrôle de la connectivité (en minutes)	Affiche le temps d'attente avant de restaurer la configuration.

Vous pouvez définir les paramètres de déploiement à partir de la page de **Device management (gestion des appareils)**. Les paramètres de déploiement comprennent l'activation de la restauration automatique du déploiement si la connexion de gestion échoue à la suite du déploiement; en particulier si vous utilisez des données pour l'accès au centre de gestion, puis si vous configurez mal l'interface de données. Vous pouvez également annuler manuellement la configuration à l'aide de la commande **configure policy rollback** (voir [Restaurer manuellement la configuration si le Centre de gestion perd la connexion, à la page 43](#)).

Consultez les consignes suivantes :

- Seul le déploiement précédent est disponible localement sur défense contre les menaces ; vous ne pouvez pas restaurer les déploiements précédents.
- La restauration est prise en charge pour la haute disponibilité mais pas pour les déploiements de mise en grappe.
- La restauration n'est pas prise en charge immédiatement après la création de la haute disponibilité.
- Le restaurer ne vise que les configurations que vous pouvez définir dans l'application centre de gestion. Par exemple, la restauration ne touche aucune configuration locale liée à l'interface de commande dédiée, que vous ne pouvez configurer qu'au niveau de l'interface de ligne de commande défense contre les menaces . Notez que si vous avez modifié les paramètres de l'interface de données après le dernier centre de gestion déploiement à l'aide de la commande **configure network management-data-interface**, et que vous utilisez ensuite la commande de restauration, ces paramètres ne seront pas conservés ; ils seront restaurés aux paramètres centre de gestion déployés en dernier lieu.
- Le mode UCAPL/CC ne peut pas être annulé.
- Les données de certificat SCEP hors bande qui ont été mises à jour lors du déploiement précédent ne peuvent pas être restaurées.
- Pendant la restauration, les connexions seront interrompues, car la configuration actuelle sera effacée.

Procédure

Étape 1 Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.

Étape 2 En regard du périphérique auquel vous souhaitez affecter des politiques, cliquez sur **Edit** (✎).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Dans la section **Deployment Settings (paramètres de déploiement)**, cliquez sur **Edit** (✎).

Illustration 34 : Paramètres de déploiement

Deployment Settings

Auto Rollback Deployment if Connectivity Fails:

Connectivity Monitor Interval (in Minutes): 20

The connectivity failure timeout will be applicable from next deployment incase, the deployment for this device is already in progress.

Cancel Save

Étape 5 Cochez la case **Auto Rollback Deployment if Connectivity Fails (déploiement de la restauration automatique en cas d'échec)** de la connectivité pour activer la restauration automatique.

Étape 6 Définissez **Connectivity Monitor Interval (l'intervalle du moniteur de connectivité, en minutes)** pour définir le temps d'attente avant la restauration de la configuration. La valeur par défaut est 20 minutes.

Étape 7 En cas de restauration, reportez-vous aux étapes suivantes pour connaître les étapes suivantes.

- Si la restauration automatique a réussi, un message de réussite s'affiche, vous demandant d'effectuer un déploiement complet.
- Vous pouvez également accéder à l'écran **Deploy > Advanced Deploy** (Déployer > Déployer de manière avancée) et cliquer sur l'icône **Preview** (📄) (Aperçu) pour afficher les parties de la configuration qui ont été rétablies (voir [Déployer les modifications de configuration](#)). Cliquez sur **Show Rollback Changes (afficher les changements restaurés)** pour afficher les modifications et sur **Hide Rollback Changes (Masquer les changements restaurés)** pour masquer les modifications.

Illustration 35 : Restaurer des modifications

Change Log: 10.10.35.97

⚠ This device requires a full deployment as auto rollback operation is performed in the device. [see more](#)
[Hide Rollback Changes](#)

Preview Changes Rollback Changes

Legend: ■ Added ■ Edited ■ Removed

Changed Policies	Deployed Version	Version on FMC	Modified By
<ul style="list-style-type: none"> Routing Virtual Router (Global) <ul style="list-style-type: none"> Static Route IPv4 Static Route IPv6 	Routing: Virtual Router: Virtual Router (Global) Static Route IPv4: IPv4 Route: Static Route Interface(Unchanged): outside outside Static Route Network(Unchanged): any-ipv4 any-ipv4 Gateway: literal:10.10.35.63 literal:10.10.35.64 Static Route IPv6: IPv6 Route: IPv6 Static Route Interface(Unchanged): inside inside IPv6 Static Route Network(Unchanged): any-ipv6 any-ipv6 IPv6 Static Route gateway: literal:20::20 literal:20::23		
			admin
			admin

Download as PDF OK

- Dans l'aperçu de l'historique de déploiement, vous pouvez afficher les modifications de restauration. Consultez [Afficher l'historique des déploiements](#).

Étape 8 Vérifiez que la connexion de gestion a été rétablie.

Dans centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils) > Device Management (gestion des appareils) > Device (appareil) > Management (gestion) > FMC Access Details (détails de l'accès FMC) > Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande `sftunnel-status-brief` pour afficher l'état de la connexion de gestion.

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez [Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 45](#).

Modifier les paramètres de surveillance de l'intégrité de la grappe

La section **Paramètres du moniteur d'intégrité de la grappe** de la page **Cluster (Grappe)** affiche les paramètres décrits dans le tableau ci-dessous.

Illustration 36 : Paramètres de surveillance de l'intégrité de la grappe

Cluster Health Monitor Settings			
Timeouts			
Hold Time			3 s
Interface Debounce Time			9000 ms
Monitored Interfaces			
Service Application			Enabled
Unmonitored Interfaces			None
Auto-Rejoin Settings			
	Attempts	Interval Between Attempts	Interval Variation
Cluster Interface	-1	5	1
Data Interface	3	5	2
System	3	5	2

Tableau 7 : Champs de la table Paramètres de surveillance de l'intégrité de la grappe

Champ	Description
Délai d'expiration	
Temps de retenue	Pour déterminer l'état de santé du système, les nœuds de la grappe envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.
Délai de l'antirebond de l'interface	L'heure de l'antirebond de l'interface est le délai avant que le nœud considère une interface comme défaillante et que le nœud ne soit retiré de la grappe.
Interfaces surveillées	La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe.
Application de service	Indique si Snort et les processus de disque plein sont surveillés.
Interfaces non surveillées	Affiche les interfaces non surveillées.
Paramètres de la jonction automatique	
Interface de la grappe	Affiche les paramètres de jonction automatique en cas d'échec de la liaison de commande de grappe.

Champ	Description
Interfaces de données	Affiche les paramètres de jonction automatique en cas de défaillance de l'interface de données.
Système	Affiche les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.



Remarque Si vous désactivez la vérification de l'intégrité du système, les champs qui ne s'appliquent pas lorsque la vérification de l'intégrité du système est désactivée ne s'afficheront pas.

Vous pouvez utiliser ces paramètres dans cette section.

Vous pouvez surveiller n'importe quel ID de canal de port, tout ID d'interface physique unique, ainsi que les processus Snort et de disque plein. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

- Étape 1** Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.
- Étape 2** À côté de la grappe que vous souhaitez modifier, cliquez sur **Edit** (✎).
- Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.
- Étape 3** Cliquez sur **Cluster** (Grappe).
- Étape 4** Dans la section **Cluster Health Monitor Settings** (paramètres de surveillance d'intégrité de la grappe), cliquez sur **Edit** (✎).
- Étape 5** Désactivez la fonction de vérification de l'intégrité du système en cliquant sur le curseur **Vérification de l'intégrité**.

Illustration 37 : Désactiver la vérification de l'intégrité du système

Edit Cluster Health Monitor Settings

Health Check ⓘ

▼ Timeouts

Hold Time Range: 0.3 to 45 seconds

Interface Debounce Time Range: 300 to 9000 milliseconds

> Auto-Rejoin Settings

> Monitored Interfaces

Reset to Defaults Cancel Save

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 6

Configurez le temps d'attente et le temps d'antirebond de l'interface.

- **Hold Time** (Temps d'attente) : permet de définir le délai d'attente pour déterminer l'intervalle de temps entre les messages d'état de pulsation du nœud, entre 0,3 et 45 secondes; La valeur par défaut est de 3 secondes.
- **Interface Debounce Time** (Temps d'antirebond de l'interface) : définit le temps d'antirebond entre 300 et 9000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, le nœud attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe de l'état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un temps d'antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe juste, car un autre nœud de la grappe a été plus rapide à regrouper les ports.

Étape 7

Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

Illustration 38 : Configurer les paramètres de jonction automatique

▼ Auto-Rejoin Settings

Cluster Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

Data Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

System

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

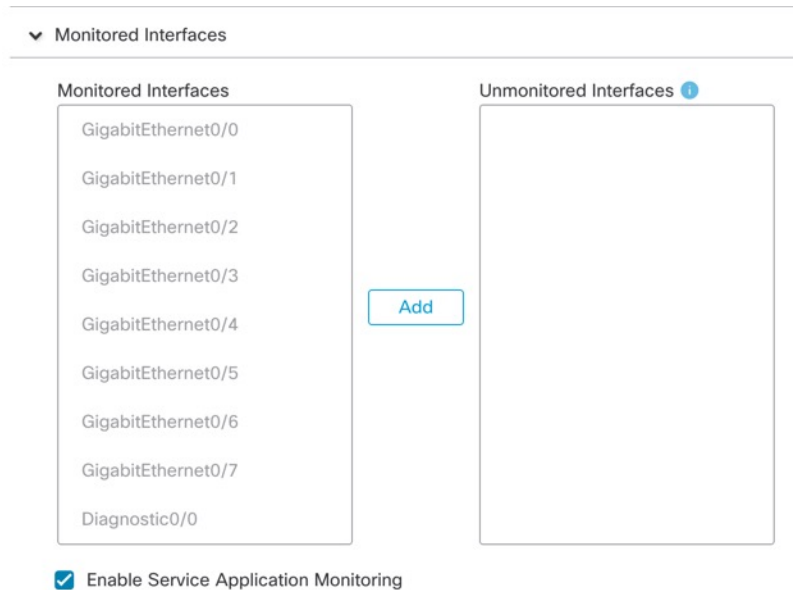
Définissez les valeurs suivantes pour l'**interface de grappe**, l'**interface de données** et le **système** (les défaillances internes comprennent : l'expiration du délai de synchronisation des applications, des états d'applications incohérents, etc.) :

- **Tentatives** – Définit le nombre de tentatives de jonction, entre -1 et 65 535. **0** désactive la jonction automatique. La valeur par défaut pour l' **interface de la grappe** est -1 (illimité). La valeur par défaut pour l'**interface de données** et le **système** est 3.
- **Interval Between Attempts** (intervalle entre les tentatives) : Permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente. définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente), ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l' **interface de grappe** et **2** pour l' **interface de données** et le **système**.

Étape 8

Configurez les interfaces surveillées en les déplaçant dans la fenêtre **Interfaces surveillées** ou **interfaces non surveillées**. Vous pouvez également cocher ou décocher la case **Enable Service Application Monitoring** (activer la surveillance des applications de service) pour activer ou désactiver la surveillance Snort et des processus de surveillance de disque plein.

Illustration 39 : configurer les interfaces surveillées



La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces et pour les processus Snort et de détection du disque plein.

Vous pouvez souhaiter désactiver la surveillance de l'état des interfaces non essentielles, par exemple l'interface de diagnostic.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 9

Cliquez sur **Save** (enregistrer).

Étape 10

Déployer les changements de configuration.

Échange à chaud d'un SSD sur Cisco Secure Firewall

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

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

**Mise en garde**

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

Procédure**Étape 1**

Retirez l'un des disques SSD.

- a) Retirez le SSD du RAID.

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

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

Exemple :

```
> configure raid remove-secure local-disk 2
```

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

show raid

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

Exemple :

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

```

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

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

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

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

```

- c) Retirez physiquement le disque SSD du châssis.

Étape 2

Ajouter un disque SSD.

- Ajoutez physiquement le SSD dans le logement vide.
- Ajoutez le SSD au RAID.

configure raid add local-disk {1 | 2}

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

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

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

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

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.