Périphériques logiques sur les appareils Firepower 4100/9300

Firepower 4100/9300 est une plateforme de sécurité flexible sur laquelle vous pouvez installer un ou plusieurs *périphériques logiques*.

Vous devez configurer les interfaces de châssis, ajouter un périphérique logique et affecter des interfaces au périphérique sur le châssis Firepower 4100/9300 à l'aide de Cisco Firepower Chassis Manager ou de la CLI FXOS. Vous ne pouvez pas effectuer ces tâches dans FDM.

Ce chapitre décrit la configuration de l'interface de base et comment ajouter un périphérique logique autonome ou à haute accessibilité à l'aide de Cisco Firepower Chassis Manager . Pour utiliser l'interface de ligne de commande de FXOS, consultez le guide de configuration de l'interface de ligne de commande FXOS. Pour des procédures FXOS et un dépannage plus avancés, consultez le guide de configuration FXOS.

À propos des interfaces

Le Châssis Firepower 4100/9300 prend en charge les interfaces physiques et les interfaces EtherChannel (canal de port). Les interfaces EtherChannel peuvent comprendre jusqu'à 16 interfaces membres du même type.

Interface de gestion de châssis

L'interface de gestionnaire de châssis est utilisée pour la gestion du châssis FXOS par SSH ou Cisco Firepower Chassis Manager. Cette interface est distincte de l'interface de type gestion (mgmt) que vous affectez aux périphériques logiques pour la gestion des applications.

Pour configurer les paramètres de cette interface, vous devez les configurer à partir de l'interface de ligne de commande. Pour afficher des informations sur cette interface dans l'interface de ligne de commande FXOS, connectez-vous à la gestion locale et affichez le port de gestion :

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

Notez que l'interface de gestion du châssis reste active même si le câble physique ou le module SFP est débranché ou que la commande **mgmt-port shut** est exécutée.

Remarque L'interface de gestion de châssis ne prend pas en charge les trames étendues.

Types d'interface

Les interfaces physiques et les interfaces EtherChannel (canal de port) peuvent être de l'un des types suivants :

- Données : à utiliser pour les données normales. Les interfaces de données ne peuvent pas être mises en commun entre les périphériques logiques, et les périphériques logiques ne peuvent pas communiquer avec d'autres périphériques logiques par le fond de panier Pour le trafic sur les interfaces de données, tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre périphérique logique.
- Data-sharing (partage de données) : à utiliser pour les données normales. Pris en charge uniquement avec les instances de conteneur, ces interfaces de données peuvent être partagées par un ou plusieurs dispositifs logiques/Instances de conteneur (Cisco Firepower Threat Defense-utilisant-FMC seulement).
- Gestion : permet de gérer les instances d'application. Ces interfaces peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique. En fonction de votre application et de votre gestionnaire, vous pouvez ultérieurement activer la gestion à partir d'une interface de données; mais vous devez attribuer une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données. Pour en savoir plus sur l'interface de gestion de châssis distincte, consultez Interface de gestion de châssis, à la page 1.

Remarque La modification de l'interface de gestion entraînera le redémarrage du périphérique logique. Par exemple, une gestion des modifications de e1/1 à e1/2 entraînera le redémarrage du périphérique logique pour appliquer la nouvelle gestion.

- Créer un événement— Sert d'interface de gestion secondaire pour les périphériques Cisco Firepower Threat Defense-using- (en usage)FMC.

Remarque Une interface Ethernet virtuelle est attribuée lors de l'installation de chaque instance applicative. Si l'application n'utilise pas d'interface événementielle, l'interface virtuelle sera dans un état "admin down".

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster (grappe) : à utiliser comme liaison de commande de grappe pour un périphérique logique en grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48. Le type de grappe est uniquement pris en charge sur les interfaces EtherChannel. Le FDM et CDO ne prend pas en charge le regroupement (clustering).

Interfaces FXOS par rapport aux interfaces d'application

Le Firepower 4100/9300 gère les paramètres Ethernet de base des interfaces physiques, les sous-interfaces VLAN pour les instances de conteneur et . Dans l'application, vous configurez les paramètres de niveau supérieur. Par exemple, vous pouvez uniquement créer des EtherChannels dans FXOS; mais vous pouvez attribuer une adresse IP à l'EtherChannel dans l'application.

Les sections suivantes décrivent l'interaction entre FXOS et l'application pour les interfaces.

Sous-interfaces VLAN

Pour tous les périphériques logiques, vous pouvez créer des sous-interfaces VLAN dans l'application.

États indépendants de l'interface dans le châssis et dans l'application

Vous pouvez activer et désactiver administrativement les interfaces dans le châssis et dans l'application. Pour qu'une interface soit opérationnelle, elle doit être activée dans les deux systèmes d'exploitation. Étant donné que l'état de l'interface est contrôlé indépendamment, il se peut que vous ayez une incompatibilité entre le châssis et l'application.

Exigences et conditions préalables pour les combinaisons matérielles et logicielles de l'appareil Firepower 9300

L'appareil Firepower 9300 comprend 3 logements pour module de sécurité et plusieurs types de modules de sécurité. Consultez les exigences suivantes :

- Security Module Types (types de modules de sécurité) : Vous pouvez installer des modules de différents types dans le périphérique Firepower 9300. Par exemple, vous pouvez installer le SM-48 comme module 1, le SM-40 comme module 2 et le SM-56 comme module 3.
- Instances natives et de conteneur : lorsque vous installez une instance de conteneur sur un module de sécurité, ce module ne peut prendre en charge que d'autres instances de conteneur. Une instance native utilise toutes les ressources d'un module, vous ne pouvez donc installer qu'une seule instance native sur un module. Vous pouvez utiliser des instances natives sur certains modules et des instances de conteneur sur les autres modules. Par exemple, vous pouvez installer une instance native sur le module 1 et le module 2, mais des instances de conteneur sur le module 3.
- High Availability (haute disponibilité) : la haute disponibilité est prise en charge uniquement entre les modules de même type sur le périphérique Firepower 9300. Cependant, les deux châssis peuvent comprendre des modules mixtes. Par exemple, chaque châssis a un SM-40, SM-48 et SM-56. Vous pouvez créer des paires à haute disponibilité entre les modules SM-40, entre les modules SM-48 et entre les modules SM-56.

- Types d'applications ASA et FTD :Vous pouvez installer différents types d'applications sur des modules distincts dans le châssis. Par exemple, vous pouvez installer ASA sur le module 1 et le module 2, et FTD sur le module 3.
- Versions ASA ou FTD : vous pouvez exécuter différentes versions d'un type d'instance d'application sur des modules distincts ou en tant qu'instances de conteneur distinctes sur le même module. Par exemple, vous pouvez installer FTD 6.3 sur le module 1, FTD 6.4 sur le module 2 et FTD 6.5 sur le module 3.

Lignes directrices et limites relatives aux périphériques logiques

Consultez les sections suivantes pour connaître les instructions et les limites.

Lignes directrices et limites des interfaces

Adresses MAC par défaut

Les attributions d'adresses MAC par défaut dépendent du type d'interface.

- Interfaces physiques : l'interface physique utilise l'adresse MAC gravée.
- EtherChannels : Pour un EtherChannel, toutes les interfaces du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels. L'interface du canal de port utilise une adresse MAC unique provenant d'un pool; L'appartenance à l'interface n'affecte pas l'adresse MAC.

Lignes directrices et limites générales

Haute disponibilité

- Configurez la haute disponibilité dans la configuration de l'application.
- Vous pouvez utiliser n'importe quelle interface de données comme liens de basculement et d'état.
- Les deux unités d'une configuration de basculement à haute accessibilité doivent :
  - être du même modèle.
  - Avoir les mêmes interfaces que celles des périphériques logiques à haute accessibilité.
  - Avoir le même nombre et les mêmes types d'interfaces. Toutes les interfaces doivent être préconfigurées de manière identique dans FXOS avant que vous activiez la haute accessibilité.
- Pour en savoir plus, consultez Configuration requise pour la haute accessibilité.

Interfaces de configuration

Par défaut, les interfaces physiques sont désactivées. Vous pouvez activer les interfaces, ajouter des canaux EtherChannels, et modifier les propriétés de l'interface et .

Activer ou désactiver une interface

Vous pouvez modifier l' **état d'administration** de chaque interface pour l'activer ou la désactiver. Par défaut, les interfaces physiques sont désactivées.

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page Interfaces présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Pour activer l'interface, cliquez sur le bouton désactivé **Curseur désactivé** () pour qu'il devienne activé **Curseur activé** ().

Cliquez sur **Yes** (oui) pour confirmer la modification. L'interface correspondante dans la représentation visuelle passe du gris au vert.

Étape 3 Pour désactiver l'interface, cliquez sur le **Curseur activé** () activé pour qu'elle devienne désactivée **Curseur désactivé** ().

Cliquez sur **Yes** (oui) pour confirmer la modification. L'interface correspondante dans la représentation visuelle passe du vert au gris.

Configurer une interface physique

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

Remarque Dans le cas de QSFPH40G-CUxM, la négociation automatique est toujours activée par défaut et vous ne pouvez pas la désactiver.

Avant de commencer

- Les interfaces qui sont déjà membres d'un EtherChannel ne peuvent pas être modifiées individuellement. Assurez-vous de configurer les paramètres avant de les ajouter au canal EtherChannel.

Ajouter un canal EtherChannel (canal de port)

Un EtherChannel (également appelé canal de port) peut inclure jusqu'à 16 interfaces membres de même type de support et de capacité, et doit être réglé à la même vitesse et au même duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité. Le protocole LACP (Link Aggregation Control Protocol) agrège les interfaces en échangeant les LACPDU (Link Aggregation Control Protocol Data Unit) entre deux périphériques réseau.

Vous pouvez configurer chaque interface physique de données dans un EtherChannel pour qu'elle soit :

- Actif : envoie et reçoit les mises à jour du protocole LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.
- Activé : l'EtherChannel est toujours activé et le protocole LACP n'est pas utilisé. Un EtherChannel « activé » ne peut établir une connexion qu'avec un autre EtherChannel « activé ».

Remarque Cela peut prendre jusqu'à trois minutes à un EtherChannel de revenir à l'état opérationnel si vous faites passer son mode de On (Activé) à Actif ou de Actif à Activé.

Le Châssis Firepower 4100/9300 ne prend en charge les EtherChannels qu'en mode LACP actif de sorte que chaque interface membre envoie et reçoive des mises à jour LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.

Le protocole LACP coordonne l'ajout et la suppression automatiques des liens vers l'EtherChannel sans l'intervention de l'utilisateur. Il gère également les erreurs de configuration et vérifie que les deux extrémités des interfaces membres sont connectées au groupe de canaux approprié. Le mode « Activé» ne peut pas utiliser les interfaces en veille dans le groupe de canaux lorsqu'une interface tombe en panne et que la connectivité et les configurations ne sont pas vérifiées.

Lorsque Châssis Firepower 4100/9300 crée un EtherChannel, l'EtherChannel reste dans un état **Suspendu** pour le mode LACP actif ou à l'arrêt pour le mode LACP **activé** jusqu'à ce que vous l'affectiez à un périphérique logique, même si le lien physique est actif. L'EtherChannel sortira de l'état **Suspendu** dans les situations suivantes :

- L'EtherChannel est ajouté en tant qu'interface de données ou de gestion pour un périphérique logique autonome
- L'EtherChannel est ajouté en tant qu'interface de gestion ou liaison de commande de grappe pour un périphérique logique qui fait partie d'une grappe
- L'EtherChannel est ajouté en tant qu'interface de données pour un périphérique logique qui fait partie d'une grappe et au moins une unité a rejoint la grappe

Notez que l'EtherChannel ne s'affiche pas tant que vous ne l'avez pas affecté à un périphérique logique. Si l'EtherChannel est retiré de l'unité logique ou si l'unité logique est supprimée, il repasse à l'état **Suspendu** ou **Inactif** .

Configurer un périphérique logique

Ajoutez un périphérique logique autonome ou une paire à haute disponibilité sur Châssis Firepower 4100/9300 .

Ajouter un FTD Standalone (Autonome) pour le FDM

Vous pouvez utiliser le FDM avec une instance native. Les instances de conteneur ne sont pas prises en charge. Les périphériques logiques autonomes fonctionnent seuls ou dans une paire haute accessibilité.

Avant de commencer

- Téléchargez l'image de l'application que vous souhaitez utiliser pour le périphérique logique à partir de Cisco.com), puis sur Châssis Firepower 4100/9300 .
- Configurez une interface de gestion à utiliser avec le périphérique logique. L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que le port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis
- Vous devez également configurer au moins une interface de données.
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce périphérique
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - l'adresse IP de la passerelle
  - l'adresse IP du serveur DNS
  - Nom d'hôte et le nom de domaine FTD

Procédure

Consultez le guide de configuration de FDM pour commencer à configurer votre politique de sécurité.

Ajouter une paire à haute disponibilité

La haute disponibilité FTD (également appelée basculement) est configurée dans l'application, pas dans FXOS. Toutefois, pour préparer votre châssis à la haute disponibilité, consultez les étapes suivantes.

Avant de commencer

Consultez la section Configuration requise pour la haute accessibilité.

Procédure

Étape 1 Attribuez les mêmes interfaces à chaque périphérique logique.

Étape 2 Attribuez une ou deux interfaces de données au basculement et à l'état des liens.

Ces interfaces échangent le trafic à haute disponibilité entre les deux châssis. Nous vous recommandons d'utiliser une interface de données de 10 Go pour un basculement et une liaison d'état combinés. Si vous avez des interfaces disponibles, vous pouvez utiliser des liaisons de basculement et d'état distincts; le lien d'état nécessite le plus de bande passante. Vous ne pouvez pas utiliser l'interface de type de gestion pour la liaison de basculement ou d'état. Nous vous recommandons d'utiliser un commutateur entre les châssis, afin qu'aucun autre périphérique ne se trouve sur le même segment de réseau que les interfaces de basculement.

Étape 3 Activez la haute disponibilité sur les périphériques logiques. Consultez Haute disponibilité (basculement).

Étape 4 Si vous modifiez les interfaces après avoir activé la haute disponibilité, modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

Modifier une interface sur un périphérique logique FTD

Vous pouvez allouer ou annuler l'allocation d'une interface sur le périphérique logique Cisco Firepower Threat Defense. Vous pouvez ensuite synchroniser la configuration de l'interface dans FDM.

L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration Cisco Firepower Threat Defense. Cependant, la suppression d'une interface utilisée dans votre politique de sécurité aura une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration Cisco Firepower Threat Defense, notamment les règles d'accès, la NAT, le SSL, les règles d'identité, le VPN, le serveur DHCP, etc. Les politiques qui font référence aux zones de sécurité ne sont pas touchées. Vous pouvez également modifier les membres d'un EtherChannel alloué sans affecter le périphérique logique ou nécessiter de synchronisation sur FDM.

vous pouvez migrer la configuration d'une interface à une autre avant de supprimer l'ancienne interface.

Avant de commencer

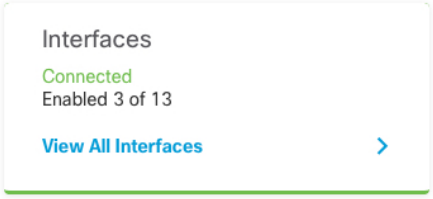
- Configurez vos interfaces et ajoutez tous les EtherChannels en fonction de Configurer une interface physique, à la page 5 et Ajouter un canal EtherChannel (canal de port), à la page 6.
- Si vous souhaitez ajouter une interface déjà allouée à un EtherChannel (par exemple, toutes les interfaces sont allouées par défaut à une grappe), vous devez d'abord désallouer l'interface du périphérique logique, puis ajouter l'interface à l'EtherChannel. Pour un nouvel EtherChannel, vous pouvez ensuite l'affecter au périphérique.
- Pour la mise en la haute disponibilité, assurez-vous d'ajouter ou de supprimer l'interface sur toutes les unités avant de synchroniser la configuration dans FDM. Nous vous recommandons d'effectuer les modifications d'interface sur l'unité de , puis sur l'unité de . Notez que les nouvelles interfaces sont ajoutées dans un état administrativement inactif, de sorte qu'elles n'affectent pas la surveillance des interfaces.

Procédure

Étape 1 Synchroniser et migrer les interfaces dans le FDM.

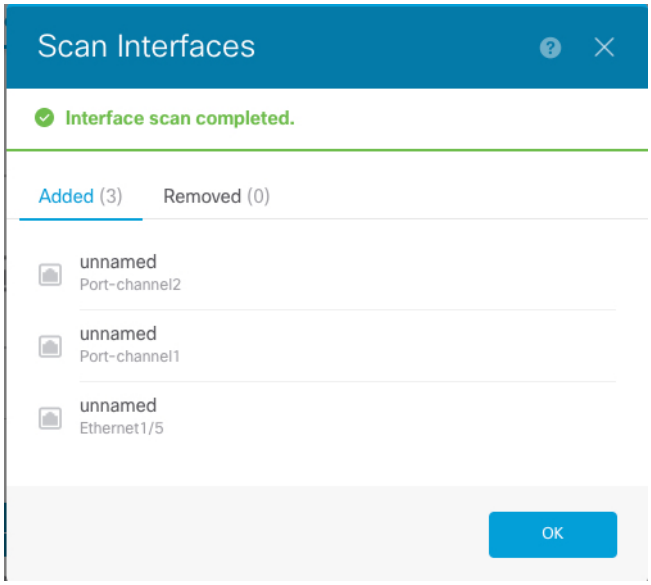
a) Connectez-vous à FDM.

b) Cliquez sur **Device** (Périphériques), puis sur le lien **View All Interfaces** (Afficher toutes les interfaces) du résume **Interfaces**.



c) Cliquez sur l'icône **Analyser les interfaces**.

d) Attendez que les interfaces effectuent l'analyse, puis cliquez sur **OK**.



e) Configurez les nouvelles interfaces avec les noms, les adresses IP, etc.

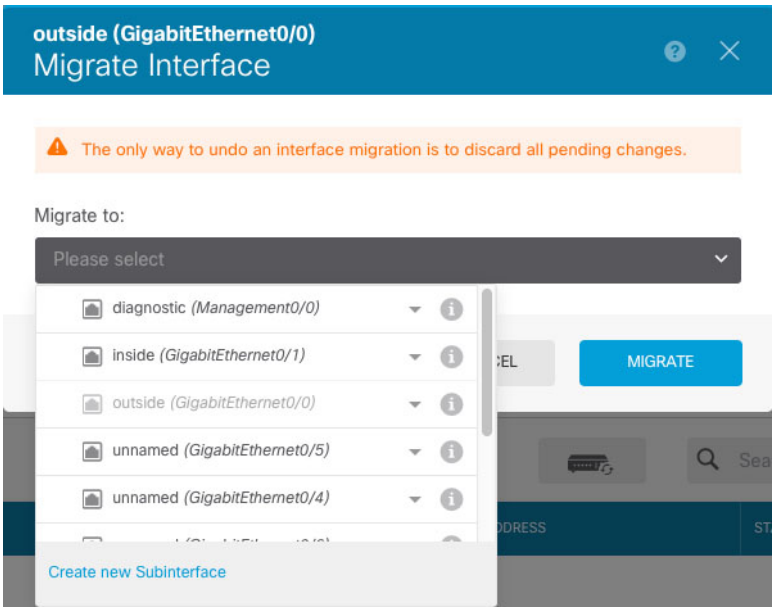
Si vous souhaitez utiliser l'adresse IP existante et le nom d'une interface que vous souhaitez supprimer, vous devez reconfigurer l'ancienne interface avec un nom et une adresse IP fictifs afin de pouvoir utiliser ces paramètres sur la nouvelle interface.

f) Pour remplacer une ancienne interface par une nouvelle interface, cliquez sur l'icône Remplacer par l'ancienne interface.

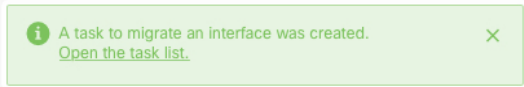
Icône Remplacer

Ce processus remplace l'ancienne interface par la nouvelle interface dans tous les paramètres de configuration qui font référence à l'interface.

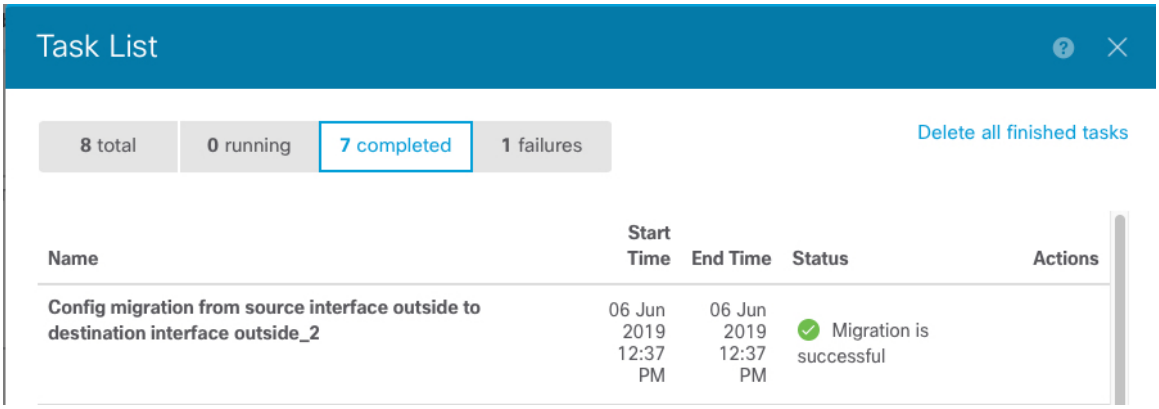
g) Choisissez la nouvelle interface dans la liste déroulante **Interface de remplacement**.



h) Un message s'affiche sur la page **Interfaces**. Cliquez sur le lien dans le message.

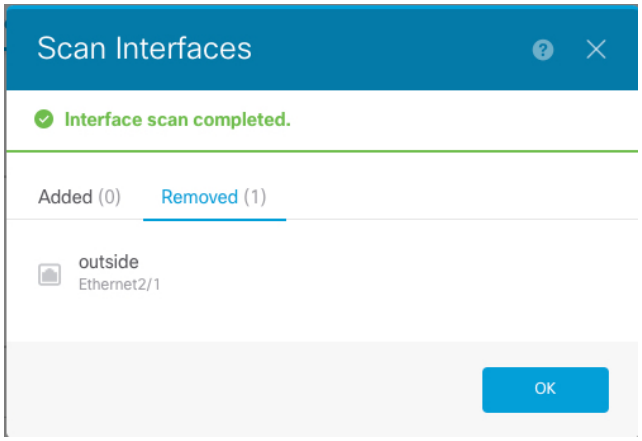


i) Vérifiez la **liste des tâches** pour vous assurer que la migration a réussi.



Étape 2 Synchronisez de nouveau les interfaces dans FDM.

Illustration 1 : Analyser les interfaces FDM



Se connecter à la console de l'application

Suivez la procédure ci-dessous pour vous connecter à la console de l'application.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

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

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

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Étape 2 Connectez-vous à la console d'application.

connect ftd *name*

Pour afficher les noms des instances, entrez la commande sans nom.

Exemple :

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

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

- FTD : Saisissez **exit**

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

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

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

Historique des dispositifs logiques Firepower 4100/9300

Fonctionnalités	Version	Détails
Prise en charge de FDM sur le Firepower 4100/9300	6.5.0	Vous pouvez maintenant utiliser les dispositifs logiques FDM avec Cisco Firepower Threat Defense sur Firepower 4100/9300. Le FDM ne prend pas en charge la capacité multi-instance ; seules les instances natives sont prises en charge. **Remarque** Nécessite FXOS 2.7.1.

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.