Configurez les services de FirePOWER sur un périphérique ISR avec une lame UCS-E

Contenu

Introduction

Ce document décrit comment installer et déployer le logiciel de Cisco FirePOWER sur une plate-forme de lame de la gamme du Système d'informatique unifiée Cisco E (UCS-E) en mode d'Instusion Detection System (ID). L'exemple de configuration qui est décrit dans ce document est un supplément au guide utilisateur officiel.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Image 3.14 des Integrated Services Router de Cisco (ISR) XE ou plus tard
- Version 2.3 ou ultérieures de Contrôleur de gestion intégré de Cisco (CIMC)
- Version 5.2 ou ultérieures du centre de Gestion de Cisco FireSIGHT (FMC)
- Version 5.2 ou ultérieures de périphérique virtuel de Cisco FirePOWER (NGIPSv)
- Version 5.0 ou ultérieures de VMware ESXi

  Note: Avant que vous amélioriez le code à la version 3.14 ou ultérieures, assurez-vous que le système a la mémoire suffisante, l'espace disque, et un permis pour la mise à jour. Référez-vous à l'exemple 1 : Copiez l'image vers le Flash : de la section Serveur TFTP du document Cisco de *procédures de mise à niveau de logiciel de Routeurs d'Access* afin de se renseigner plus sur des mises à niveau du code.

  Afin d'améliorer le CIMC, BIOS, et d'autres composants de micrologiciel, vous pouvez utiliser ou Cisco hébergez l'utilitaire de mise à jour (HUU), ou vous pouvez améliorer les composants de micrologiciel manuellement. Afin de se renseigner plus sur la mise à jour du firmware, référez-vous à améliorer le micrologiciel sur la section de serveurs de gamme E de Cisco UCS du *guide utilisateur de service de mise à jour d'hôte pour les serveurs de gamme E de Cisco UCS et l'engine de calcul de réseau de gamme E de Cisco UCS*.

Informations générales

Cette section fournit des informations au sujet des plates-formes matérielles prises en charge, permis, et limites en vue de les composants et les procédures qui sont décrits dans ce document.

Plates-formes matérielles prises en charge

Cette section répertorie les plates-formes matérielles prises en charge pour des périphériques de gammes G2 et 4000.

Périphériques d'ISR G2 avec des lames UCS-E

Ces périphériques de gamme d'ISR G2 avec des lames de gamme UCS-E sont pris en charge :

Produit	Plate-forme	Modèle UCS-E
Gamme Cisco 2900 ISR	2911	Option large simple UCS-E 120/140
	2921	Option large simple ou double UCS-E 120/140/160/180
	2951	Option large simple ou double UCS-E 120/140/160
Gamme Cisco 3900 ISR	3925	UCS-E option large simple et double de 120/140/160 ou 180 doubles larges
	3925E	UCS-E option large simple et double de 120/140/160 ou 180 doubles larges
	3945	UCS-E option large simple et double de 120/140/160 ou 180 doubles larges
	3945E	UCS-E option large simple et double de 120/140/160 ou 180 doubles larges

Périphériques ISR 4000 avec des lames UCS-E

Ces périphériques de gamme 4000 ISR avec des lames de gamme UCS-E sont pris en charge :

Produit	Plate-forme	Modèle UCS-E
Gamme Cisco 4400 ISR	4451	UCS-E option large simple et double de 120/140/160 ou 180 doubles larges
	4431	Module d'interface réseau UCS-E
Gamme Cisco 4300 ISR	4351	UCS-E option large simple et double de 120/140/160/180 ou 180 dou larges
	4331	Option large simple UCS-E 120/140
	4321	Module d'interface réseau UCS-E

Permis

L'ISR doit avoir un permis de la Sécurité K9, aussi bien qu'un permis d'*appx*, afin d'activer le service.

Limites

Voici deux limites en vue de les informations qui sont décrites dans ce document :

- La Multidiffusion n'est pas prise en charge.
- Seulement 4,096 interfaces de domaine de passerelle (BDI) sont prises en charge pour chaque système.

Le BDIs ne prennent en charge pas ces caractéristiques :

- Protocole bidirectionnel de détection d'expédition (BFD)
- NetFlow
- Qualité de service (QoS)
- Reconnaissance d'application fondée sur le réseau (NBAR) ou codage visuel avancé (AVC)
- La zone a basé le Pare-feu (ZBF)

- VPN cryptographiques
- Commutation multiprotocole par étiquette (MPLS)
- Protocole point à point (PPP) au-dessus des Ethernets (PPPoE)

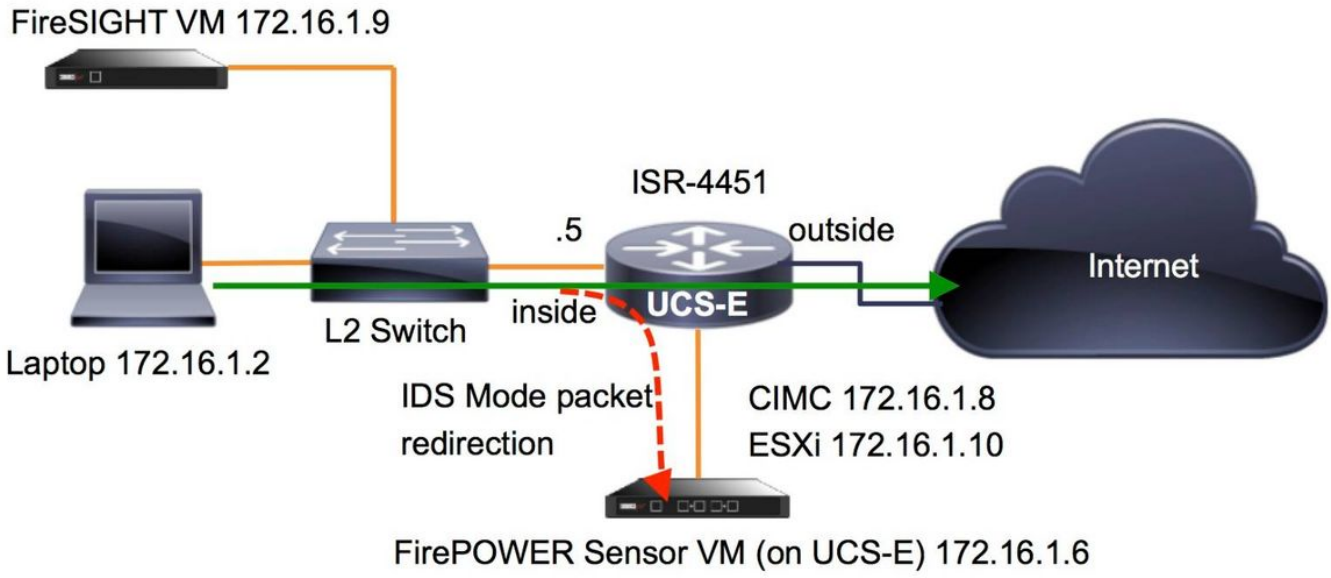
  Note: Pour un BDI, la taille de Maximum Transmission Unit (MTU) peut être configurée avec n'importe quelle valeur entre 1,500 et 9,216 octets.

Configurez

Cette section décrit comment configurer les composants qui sont impliqués de ce déploiement.

Diagramme du réseau

La configuration qui est décrite dans ce document utilise cette topologie du réseau :



Processus pour des services de FirePOWER sur UCS-E

Voici le processus pour des services de FirePOWER ce passage sur un UCS-E :

1. Les poussers de plan de données trafiquent pour l'inspection de l'interface BDI/UCS-E (travaux pour des périphériques de gammes G2 et G3).
2. Le Cisco IOS XE CLI lance la redirection de paquet pour l'analyse (options pour toutes les interfaces ou par-interface).
3. Le script de démarrage d'*installation* CLI de capteur simplifie la configuration.

Configurez le CIMC

Cette section décrit comment configurer le CIMC.

Connectez au CIMC

Il y a de plusieurs manières de se connecter au CIMC. Dans cet exemple, la connexion au CIMC est terminée par l'intermédiaire d'un port de gestion dédié. Assurez-vous que vous connectez le port **M** (dédié) au réseau à l'utilisation d'un câble Ethernet. Une fois que connecté, sélectionnez la commande de **subslot de hw-module de la** demande de routeur :

```
ISR-4451#hw-module subslot 2/0 session imc

IMC ACK: UCSE session successful for IMC
Establishing session connect to subslot 2/0
To exit, type ^a^q

picocom v1.4

port is : /dev/ttyDASH1
flowcontrol : none
baudrate is : 9600
parity is : none
databits are : 8
escape is : C-a
noinit is : no
noreset is : no
nolock is : yes
send_cmd is : ascii_xfr -s -v -l10
receive_cmd is : rz -vv

Terminal ready
```

> **Conseil** : Afin de quitter, écrivez **^a^q.**

Configurez le CIMC

Employez ces informations afin de se terminer la configuration du CIMC :

```
Unknown# scope cimc
Unknown /cimc # scope network
Unknown /cimc/network # set dhcp-enabled no
Unknown /cimc/network *# set dns-use-dhcp no
Unknown /cimc/network *# set mode dedicated
Unknown /cimc/network *# set v4-addr 172.16.1.8
Unknown /cimc/network *# set v4-netmask 255.255.255.0
Unknown /cimc/network *# set v4-gateway 172.16.1.1
Unknown /cimc/network *# set preferred-dns-server 64.102.6.247
Unknown /cimc/network *# set hostname 4451-UCS-E
Unknown /cimc/network *# commit
```

> **Attention** : Assurez-vous que vous sélectionnez la commande de **validation** afin de sauvegarder les modifications.

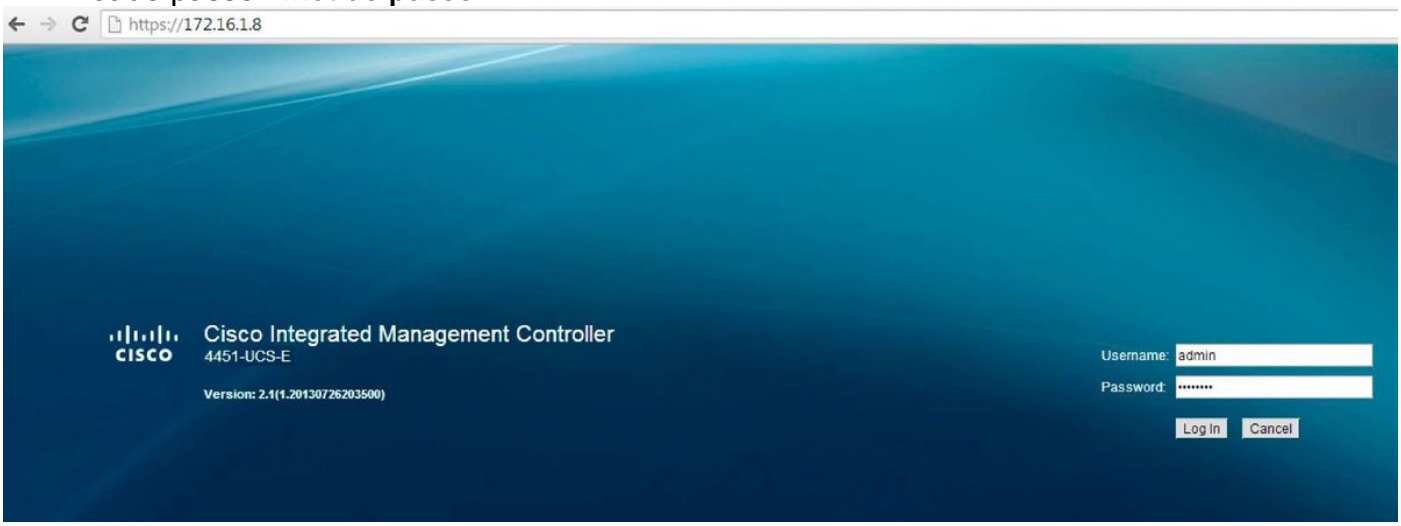
> **Note**: *Le mode* est placé **dédié** quand le port de gestion est utilisé.

Sélectionnez la commande de **détail d'exposition** afin de vérifier les configurations de détail :

```
4451-UCS-E /cimc/network # show detail
Network Setting:
IPv4 Address: 172.16.1.8
IPv4 Netmask: 255.255.255.0
IPv4 Gateway: 172.16.1.1
DHCP Enabled: no
Obtain DNS Server by DHCP: no
Preferred DNS: 64.102.6.247
Alternate DNS: 0.0.0.0
VLAN Enabled: no
VLAN ID: 1
VLAN Priority: 0
Hostname: 4451-UCS-E
MAC Address: E0:2F:6D:E0:F8:8A
NIC Mode: dedicated
NIC Redundancy: none
NIC Interface: console
4451-UCS-E /cimc/network #
```

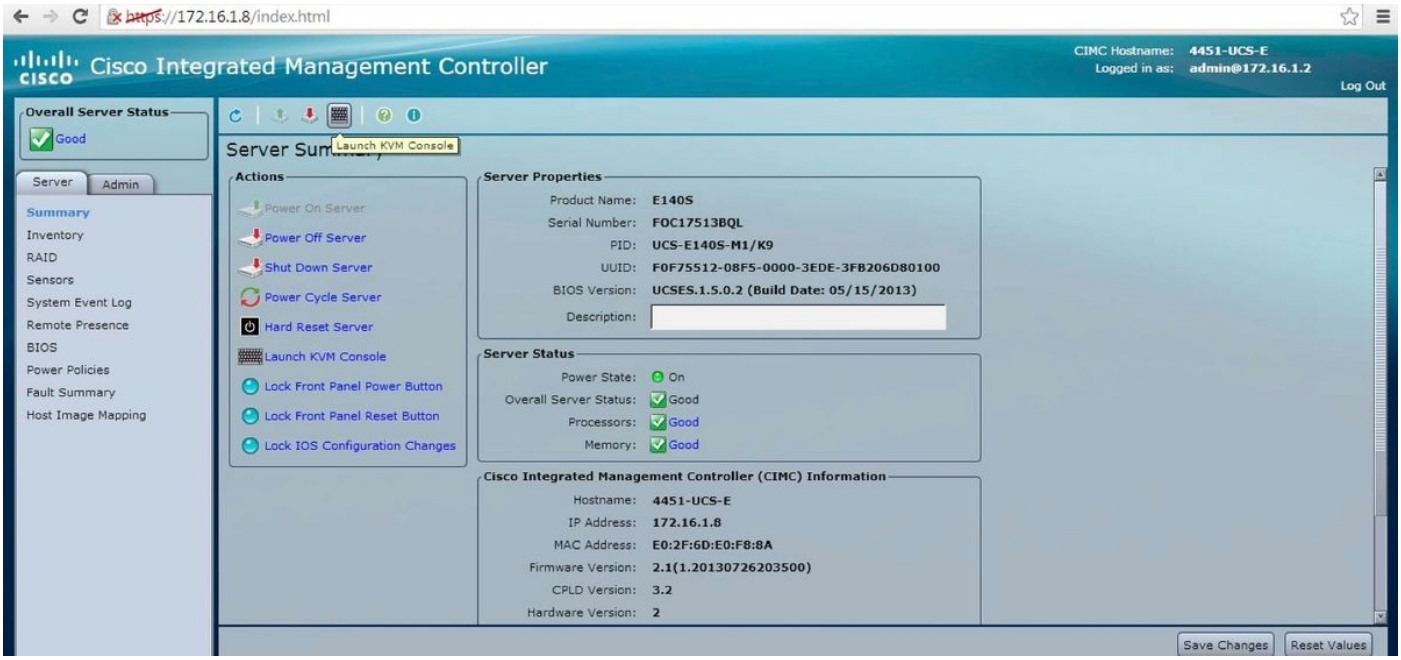
Lancez l'interface web du CIMC d'un navigateur avec le nom d'utilisateur et mot de passe par défaut. Le nom d'utilisateur et mot de passe par défaut sont :

- Nom d'utilisateur : **admin**
- Mot de passe : **mot de passe**

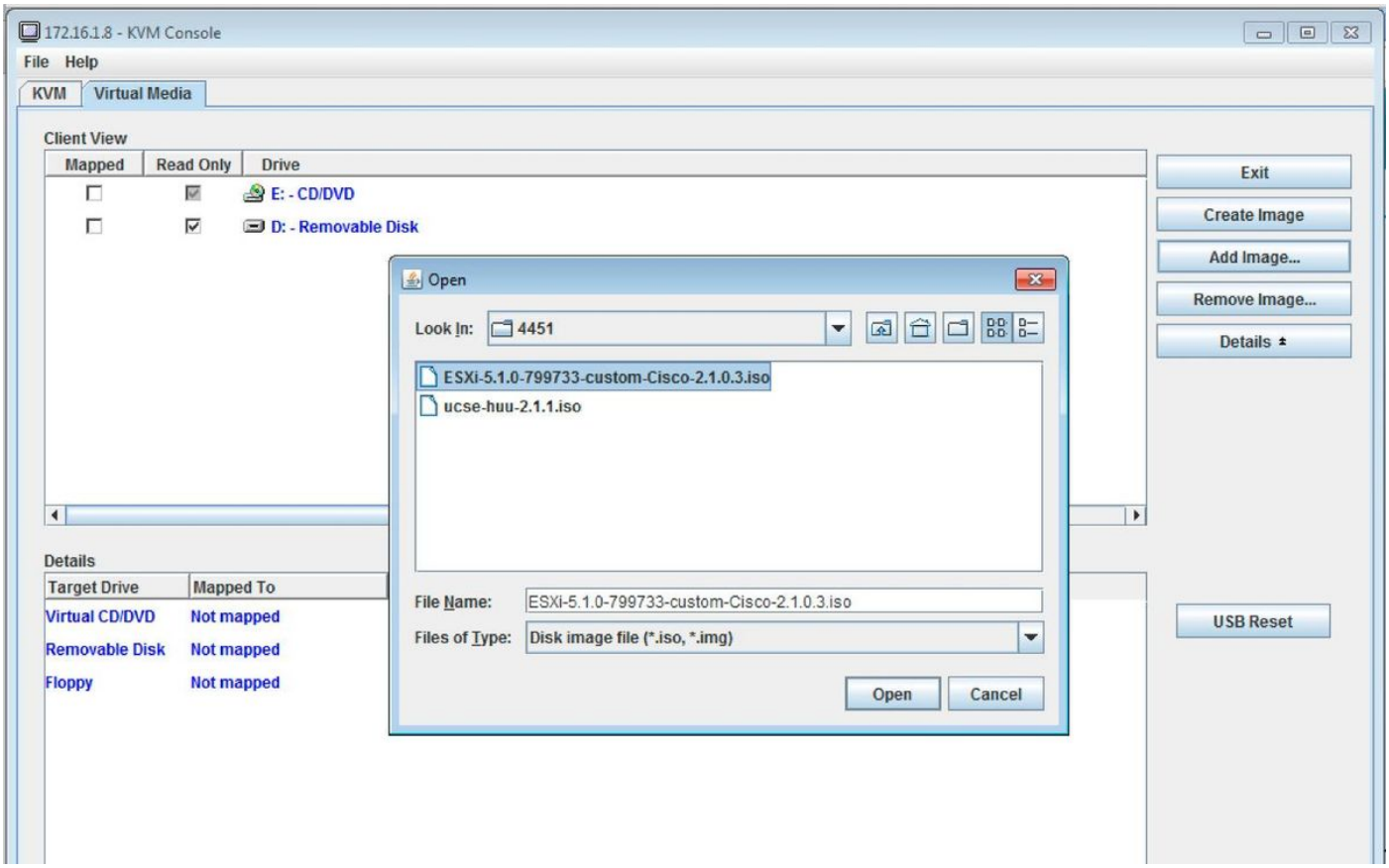


Installez ESXi

Après que vous vous connectiez dans l'interface utilisateur du CIMC, vous pouvez visualiser une page semblable à cela affichée dans la prochaine image. Cliquez sur l'icône de **console du lancement KVM**, le clic **ajoutent l'image**, et puis tracent l'OIN d'ESXi comme medias virtuels :



Cliquez sur l'onglet **virtuel de medias**, et puis cliquez sur Add l'**image** afin de tracer les medias virtuels :



Après que le support virtuel soit tracé, cliquez sur le **serveur d'arrêt et redémarrage de l'**arrêt et redémarrage de la page d'accueil CIMC l'UCS-E. Les lancements d'installation d'ESXi des medias virtuels. Terminez-vous l'ESXi installent.

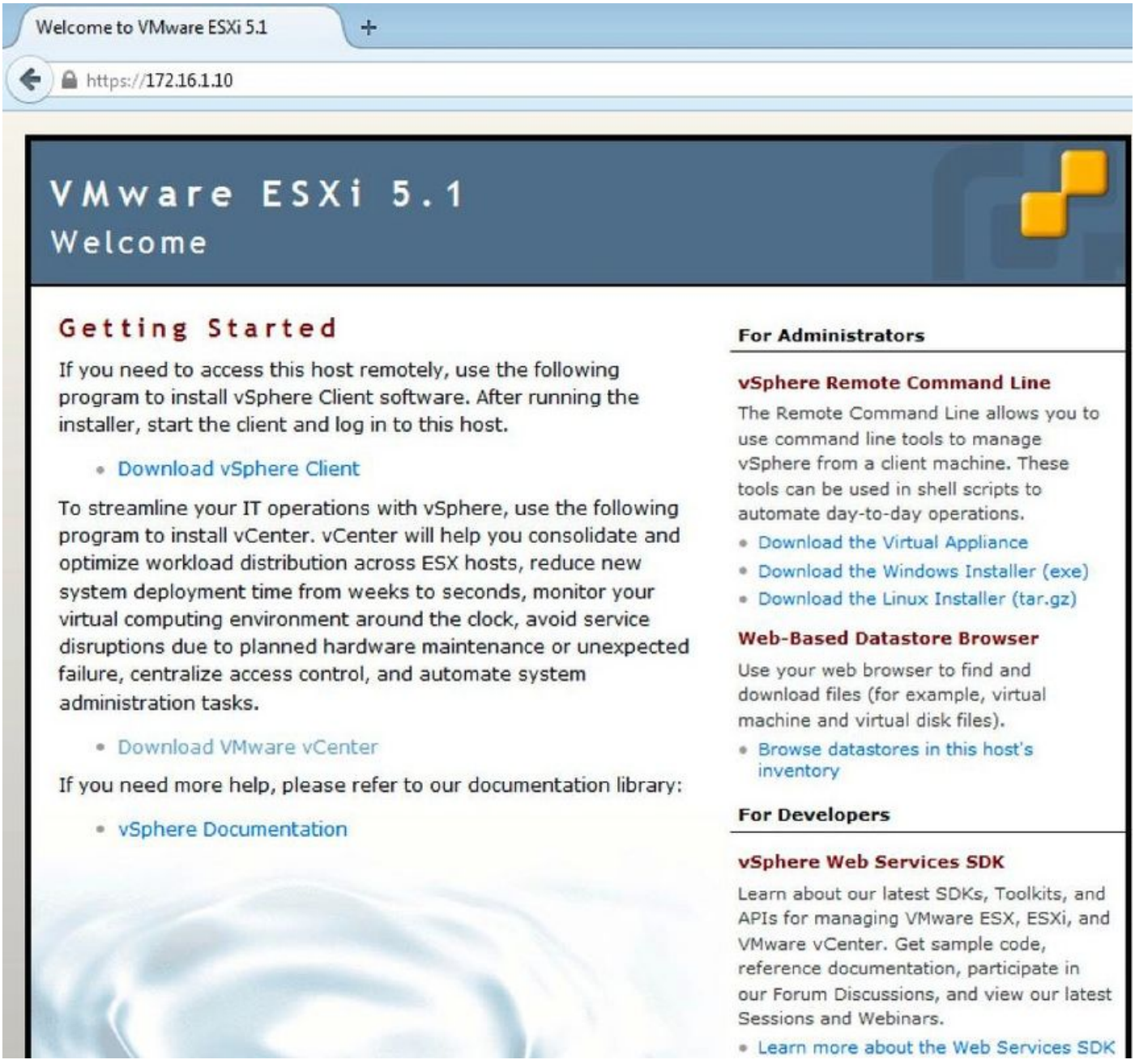
> **Note**: Enregistrez l'*adresse IP*, le *nom d'utilisateur*, et le *mot de passe d'ESXi* pour la référence ultérieure.

Installez le client de vSphere

Cette section décrit comment installer le client de vSphere.

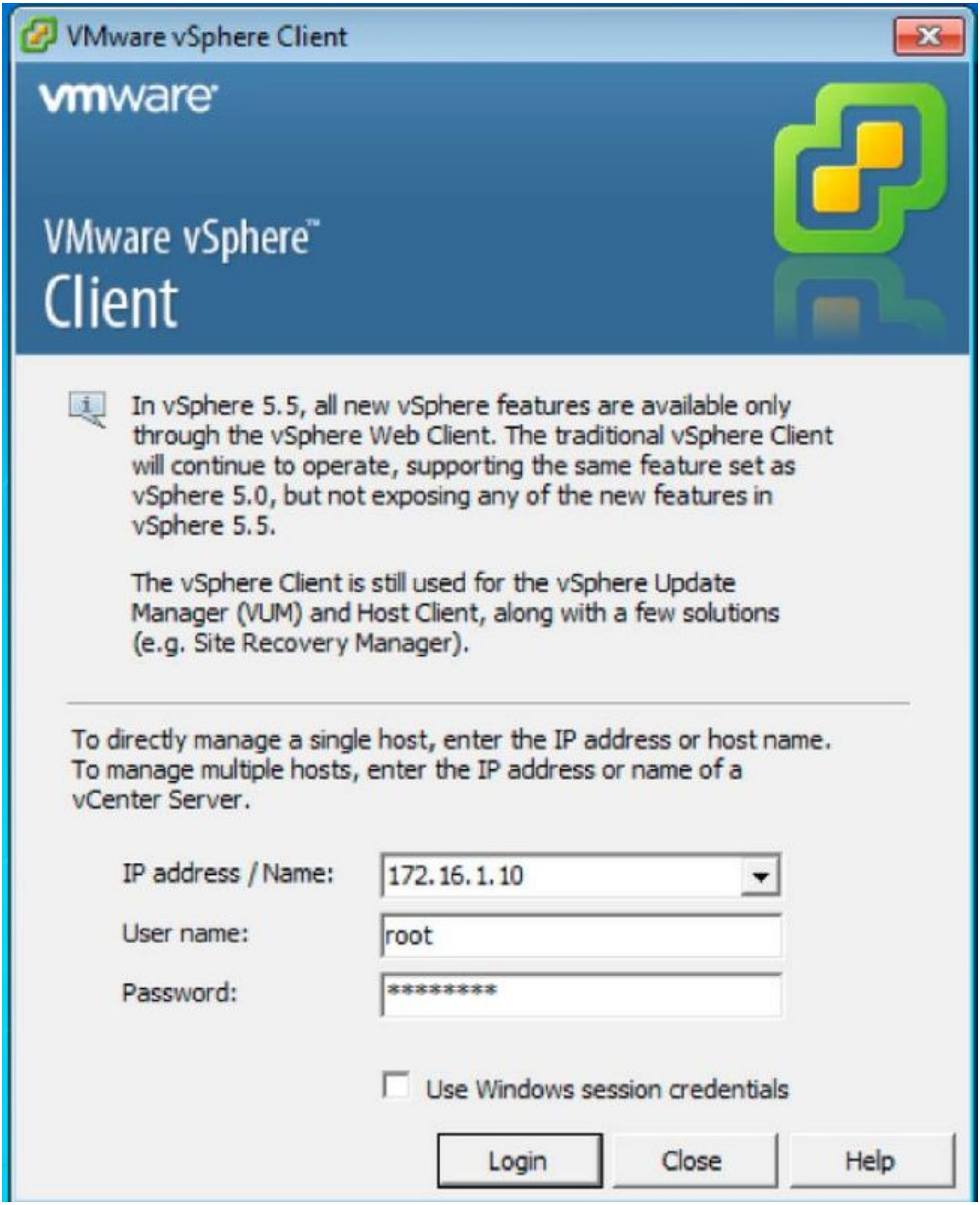
Téléchargez le client de vSphere

Lancez ESXi et employez le lien de **client de VSphere de téléchargement** afin de télécharger le client de vSphere. Installez-le sur votre ordinateur.



Lancez le client de vSphere

Lancez le client de vSphere à partir de votre ordinateur. Ouvrez une session avec le nom d'utilisateur et mot de passe que vous avez créé pendant l'installation :



Déployez le centre de Gestion de FireSIGHT et les périphériques de FirePOWER

Remplissez les procédures qui sont décrites dans le déploiement du centre de Gestion de FireSIGHT sur le document Cisco d'ESXi de VMware afin de déployer un centre de Gestion de FireSIGHT sur l'ESXi.

Note: Le processus qui est utilisé afin de déployer un périphérique de FirePOWER NGIPSv est semblable au processus qui est utilisé afin de déployer un centre de Gestion.

Configurez les interfaces

Sur l'UCS-E de la taille double, il y a quatre interfaces :

- L'interface d'adresse MAC la plus élevée est Gi3 sur le panneau avant.
- La deuxième interface d'adresse MAC la plus élevée est Gi2 sur le panneau avant.
- Les deux derniers qui apparaissent sont les interfaces internes.

Sur l'UCS-E de la taille simple, il y a trois interfaces :

- L'interface d'adresse MAC la plus élevée est Gi2 sur le panneau avant.
- Les deux derniers qui apparaissent sont les interfaces internes.

Chacun des deux interfaces UCS-E sur l'ISR4K sont des ports de joncteur réseau.

Les UCS-E 120S et 140S ont trois Network Adaptor plus des ports de gestion :

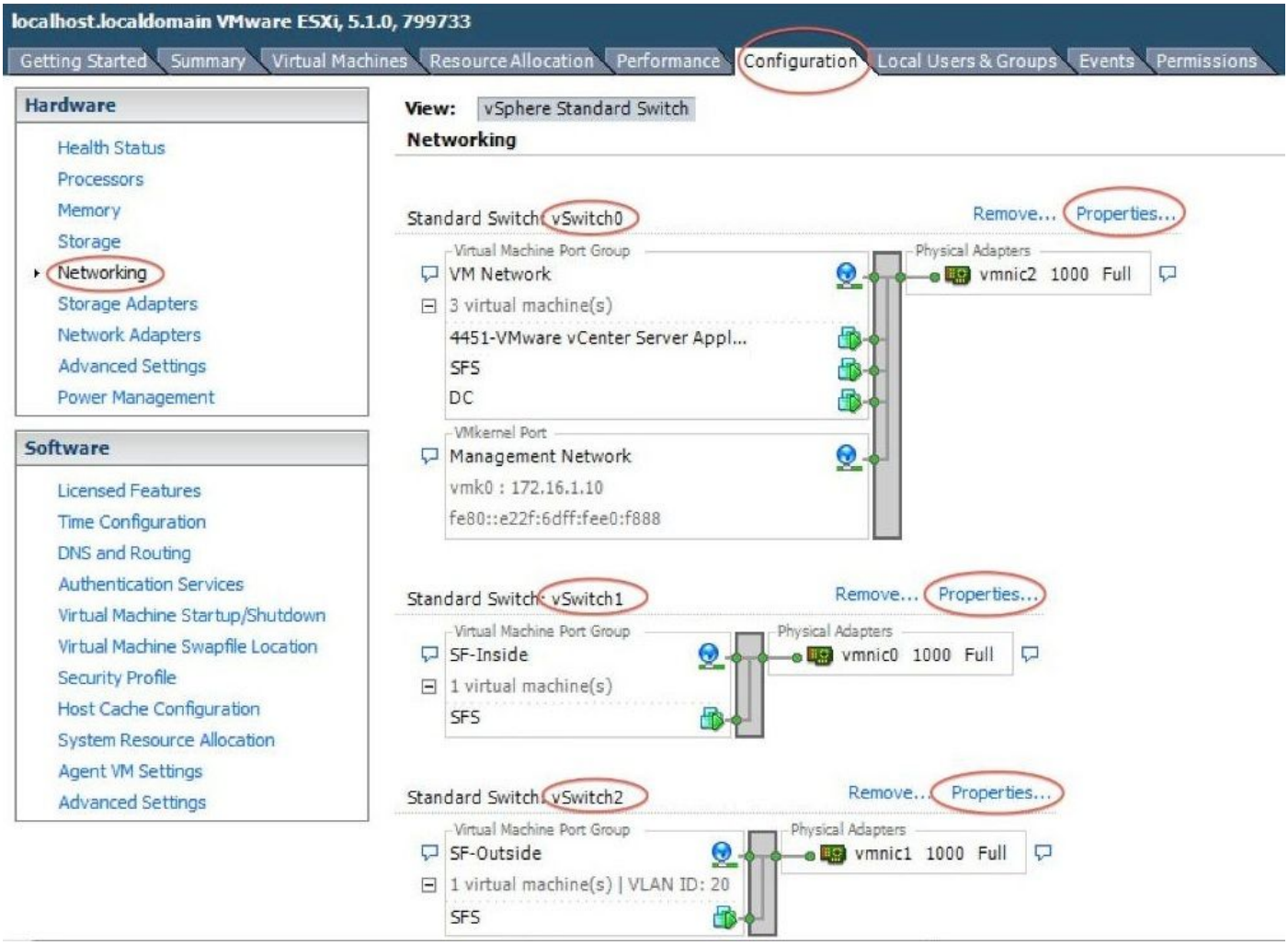
- *Le vmnic0* est tracé à *UCSEx/0/0* sur le fond de panier de routeur.
- *Le vmnic1* est tracé à *UCSEx/0/1* sur le fond de panier de routeur.
- *Le vmnic2* est tracé à l'interface de l'avion GE2 d'avant UCS-E.
- Le port de la Gestion de panneau avant (m) peut seulement être utilisé pour le CIMC.

Les UCS-E 140D, 160D, et 180D ont quatre adaptateurs réseau :

- *Le vmnic0* est tracé à *UCSEx/0/0* sur le fond de panier de routeur.
- *Le vmnic1* est tracé à *UCSEx/0/1* sur le fond de panier de routeur.
- *Le vmnic2* est tracé à l'interface de l'avion GE2 d'avant UCS-E.
- *Le vminc3* est tracé à l'interface de l'avion GE3 d'avant UCS-E.
- Le port de la Gestion de panneau avant (m) peut seulement être utilisé pour le CIMC.

Configurez les interfaces de vSwitch sur l'ESXi

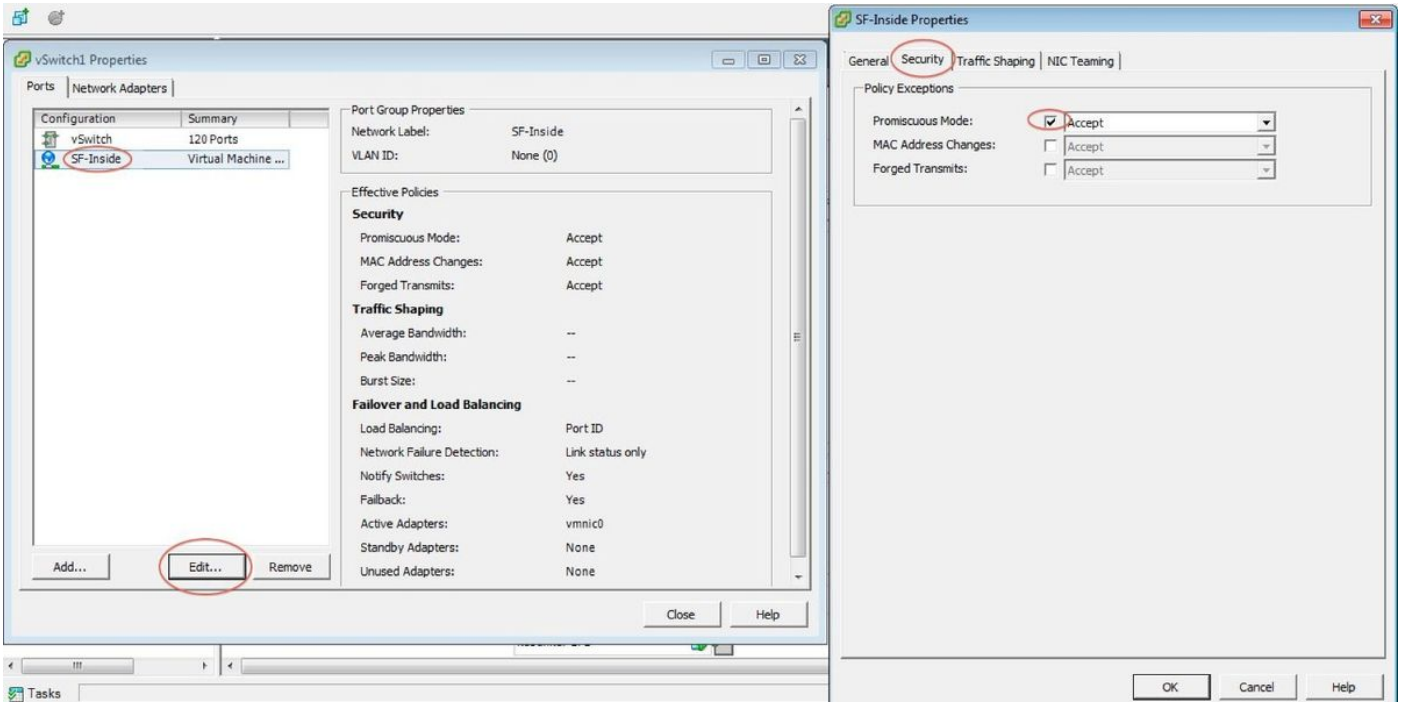
Le vSwitch0 sur l'ESXi est l'interface de gestion par laquelle l'ESXi, le centre de Gestion de FireSIGHT, et le périphérique de FirePOWER NGIPSv communiquent au réseau. Clic **Properties** pour le vSwitch1 (SF-à l'intérieur de) et le vSwitch2 (SF-extérieur) afin d'apporter à quels des modifications.



Cette image affiche les propriétés du vSwitch1 (vous devez se terminer les mêmes étapes pour le vSwitch2) :

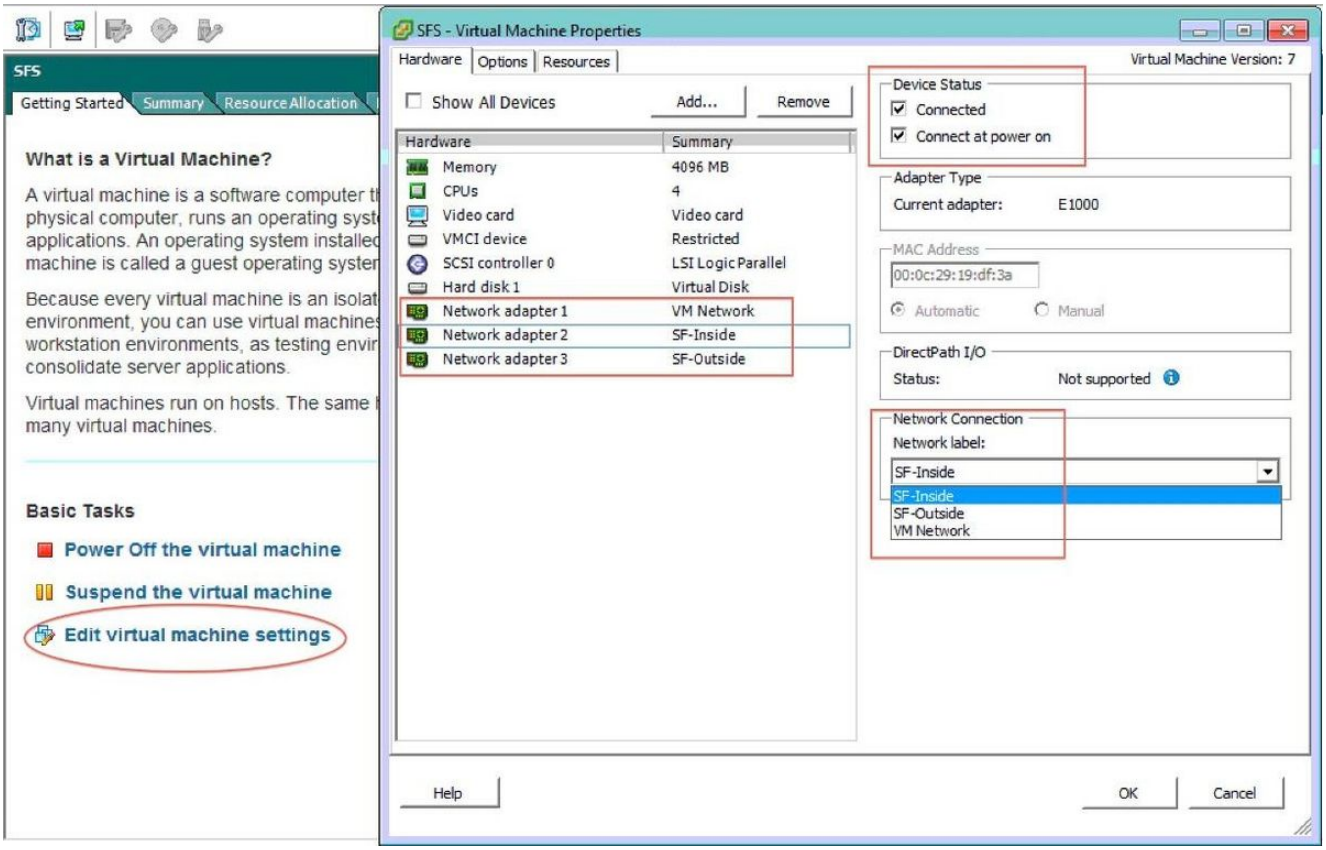
NOTE: Assurez s'il vous plaît que l'ID DE VLAN est configuré à 4095 pour NGIPSv, ceci est exigé selon le document de NGIPSv :

http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



La configuration de vSwtich sur l'ESXi est complète. Maintenant vous devez vérifier les paramètres d'interface :

1. Naviguez vers le virtual machine pour le périphérique de FirePOWER.
2. Cliquez sur Edit les **configurations de virtual machine**.
3. Vérifiez tous les trois adaptateurs réseau.
4. Assurez-vous qu'ils sont correctement choisis, comme affiché ici :



Enregistrez le périphérique de FirePOWER avec le centre de Gestion de FireSIGHT

Remplissez les procédures qui sont décrites dans le document Cisco afin d'enregistrer un périphérique de FirePOWER avec un centre de Gestion de FireSIGHT.

Réorientez et vérifiez le trafic

Cette section décrit comment réorienter le trafic et comment vérifier les paquets.

Réorientez le trafic de l'ISR au capteur sur l'UCS-E

Employez ces informations afin de réorienter le trafic :

```
interface GigabitEthernet0/0/1
ip address dhcp
negotiation auto
!
interface ucse2/0/0
no ip address
no negotiation auto
switchport mode trunk
no mop enabled
no mop sysid
service instance 1 ethernet
encapsulation untagged
bridge-domain 1
!
interface BDI1
ip unnumbered GigabitEthernet0/0/1
end
```

```
!
utd
mode ids-global
ids redirect interface BDI1
```

> **Note**: Si vous exécutez actuellement la version 3.16.1 ou ultérieures, utilisez la commande **avancée par engine UTD** au lieu de la commande **UTD**.

Vérifiez la redirection de paquet

De la console ISR, sélectionnez cette commande afin de vérifier si les compteurs de paquet incrémentent :

```
cisco-ISR4451#  show plat hardware qfp active feature utd stats

Drop Statistics:
Stats were all zero
General Statistics:
Pkts Entered Policy 6
Pkts Entered Divert 6
Pkts Entered Recycle Path 6
Pkts already diverted 6
Pkts replicated 6
Pkt already inspected, policy check skipped 6
Pkt set up for diversion 6
```

Vérifiez

Vous pouvez employer ces **commandes show** afin de vérifier que votre configuration fonctionne correctement :

- **l'exposition plat UTD de logiciel global**
- **l'exposition plat des interfaces UTD de logiciel**
- **l'exposition plat global actif UTD RP de logiciel**
- **l'exposition plat global actif point de gel UTD de logiciel**
- **l'exposition plat des stats actifs UTD de caractéristique de qfp de matériel**
- **UTD actif de caractéristique de qfp de matériel de show platform**

Dépannez

Vous pouvez employer ces commandes de **débogage** afin de dépanner votre configuration :

- **mettez au point le controlplane UTD de caractéristique d'état de plate-forme**
- **mettez au point le sous-mode de dataplane UTD de caractéristique d'état de plate-forme**

Informations connexes

- En obtenant le guide de démarrage pour les serveurs de gamme E de Cisco UCS et l'engine de calcul de réseau de gamme E de Cisco UCS, libérez 2.x
- Guide de dépannage pour les serveurs de gamme E de Cisco UCS et l'engine de calcul de réseau de gamme E de Cisco UCS
- En obtenant le guide de démarrage pour les serveurs de gamme E de Cisco UCS et l'engine de calcul de réseau de gamme E de Cisco UCS, libérez 2.x – évolution du micrologiciel
- Guide de configuration du logiciel de Routeurs à services d'agrégation de la gamme Cisco ASR 1000 – Configuration des interfaces de domaine de passerelle
- Guide utilisateur de service de mise à jour d'hôte pour les serveurs de gamme E de Cisco UCS et l'engine de calcul de réseau de gamme E de Cisco UCS – évolution du micrologiciel sur des serveurs de gamme E de Cisco UCS
- Support et documentation techniques - Cisco Systems