Configurer les services FirePOWER sur un périphérique ISR avec la lame UCS-E

Contenu

Introduction

Ce document décrit comment installer et déployer le logiciel Cisco FirePOWER sur une plate-forme lame Cisco Unified Computing System E (UCS-E) en mode IDS (Intrusion Detection System). L'exemple de configuration décrit dans ce document est un complément au guide d'utilisation officiel.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Image XE 3.14 ou ultérieure des routeurs à services intégrés Cisco (ISR)
- Cisco Integrated Management Controller (CIMC) version 2.3 ou ultérieure
- Cisco FireSIGHT Management Center (FMC) version 5.2 ou ultérieure
- Cisco FirePOWER Virtual Device (NGIPSv) version 5.2 ou ultérieure
- VMware ESXi version 5.0 ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

> **Note**: Avant de mettre à niveau le code vers la version 3.14 ou ultérieure, assurez-vous que le système dispose de suffisamment de mémoire, d'espace disque et d'une licence pour la mise à niveau. Reportez-vous à l'exemple 1 : Copiez l'image vers le Flash : de la section serveur TFTP du document Cisco Procédures de mise à niveau logicielle des routeurs d'accès afin d'en savoir plus sur les mises à niveau de code.

> **Note**: Afin de mettre à niveau CIMC, le BIOS et d'autres composants du micrologiciel, vous pouvez utiliser l'utilitaire de mise à niveau de l'hôte Cisco (HUU) ou mettre à niveau les composants du micrologiciel manuellement. Pour en savoir plus sur la mise à niveau du micrologiciel, reportez-vous à la section Mise à niveau du micrologiciel sur les serveurs Cisco UCS E du Guide d'utilisation de l'utilitaire de mise à niveau d'hôte pour les serveurs Cisco UCS E et le moteur de calcul réseau Cisco UCS E.

Informations générales

Cette section fournit des informations sur les plates-formes matérielles, les licences et les limitations prises en charge en ce qui concerne les composants et les procédures décrits dans ce document.

Plates-formes matérielles prises en charge

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

Périphériques ISR G2 avec lames UCS-E

Ces périphériques ISR G2 avec lames UCS E sont pris en charge :

Product (produit)	Plateforme	Modèle UCS-E
ISR de la gamme Cisco 2900	2911	UCS-E 120/140, option simple largeur
	2921	UCS-E 120/140/160/180, option simple ou double largeur
	2951	UCS-E 120/140/160, option simple ou double largeur
ISR de la gamme Cisco 3900	3925	UCS-E 120/140/160 option simple et double largeur ou 180 doub largeur
	3925E	UCS-E 120/140/160 option simple et double largeur ou 180 doub largeur
	3945	UCS-E 120/140/160 option simple et double largeur ou 180 doub largeur
	3945E	UCS-E 120/140/160 option simple et double largeur ou 180 doub largeur

Périphériques ISR 4000 avec lames UCS-E

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

Product (produit)	Plateforme	Modèle UCS-E
ISR de la gamme Cisco 4400	4451	UCS-E 120/140/160 option simple et double largeur ou 180 double largeur
	4431	Module d'interface réseau UCS-E
ISR de la gamme Cisco 4300	4351	UCS-E 120/140/160/180 option simple et double largeur ou 180 opt double largeur
	4331	UCS-E 120/140, option simple largeur
	4321	Module d'interface réseau UCS-E

Licences

Le routeur de service intégré doit disposer d'une licence de sécurité K9, ainsi que d'une licence appx, pour activer le service.

Limites

Voici les deux limitations relatives aux informations décrites dans ce document :

- La multidiffusion n'est pas prise en charge
- Seuls 4 096 BDI (Bridge Domain Interfaces) sont pris en charge pour chaque système

Les BDI ne prennent pas en charge ces fonctionnalités :

- Protocole BFD (Bidirectional Forwarding Detection)
- Netflow
- Quality of Service (QoS)
- NBAR (Network-Based Application Recognition) ou AVC (Advanced Video Coding)
- ZBF (Zone Based Firewall)
- VPN cryptographiques
- Commutation multiprotocole par étiquette (MPLS)
- PPP (Point-to-Point Protocol) sur Ethernet (PPPoE)

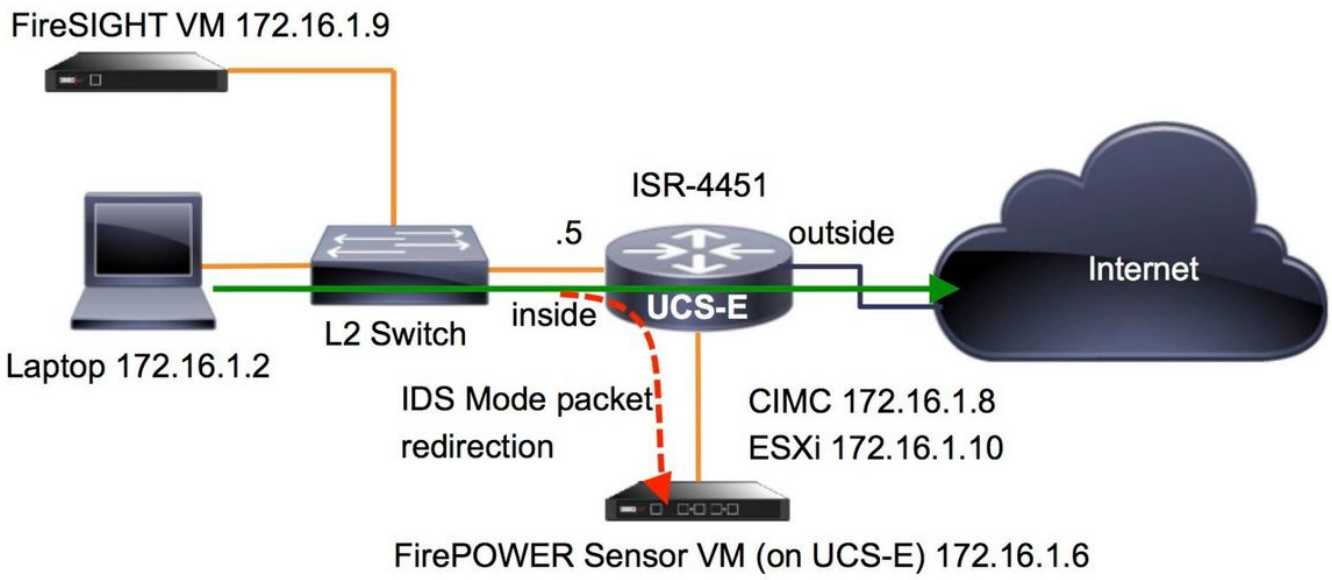
Note: Pour un BDI, la taille MTU (Maximum Transmission Unit) peut être configurée avec une valeur comprise entre 1 500 et 9 216 octets.

Configuration

Cette section décrit comment configurer les composants impliqués dans ce déploiement.

Diagramme du réseau

La configuration décrite dans ce document utilise cette topologie de réseau :



Workflow pour les services FirePOWER sur UCS-E

Voici le workflow des services FirePOWER qui s'exécutent sur UCS-E :

1. Le plan de données pousse le trafic pour inspection depuis l'interface BDI/UCS-E (fonctionne pour les périphériques G2 et G3).
2. L'interface de ligne de commande Cisco IOS®-XE active la redirection de paquets pour analyse (options pour toutes les interfaces ou par interface).
3. Le script de démarrage de **configuration** CLI du capteur simplifie la configuration.

Configurer CIMC

Cette section décrit comment configurer le CIMC.

Connexion à CIMC

Il existe plusieurs façons de se connecter au CIMC. Dans cet exemple, la connexion au CIMC est effectuée via un port de gestion dédié. Assurez-vous de connecter le port **M** (dédié) au réseau à l'aide d'un câble Ethernet. Une fois connecté, exécutez la commande **hw-module subslot** à partir de l'invite du 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 1 : Pour quitter, exécutez **^a^q**.

Conseil 2 : Le nom d'utilisateur par défaut est **admin** et le mot de passe <password>. Le processus de réinitialisation du mot de passe est décrit ici : https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/3-1-1/gs/guide/b_Getting_Started_Guide/b_3_x_Getting_Started_Guide_appendix_01011.html#GUID-73551F9A-4C79-4692-838A-F99C80E20A28

Configurer CIMC

Utilisez ces informations afin de 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 d'exécuter la commande **commit** afin d'enregistrer les modifications.

Note: Le mode est défini sur **dédié** lorsque le port de gestion est utilisé.

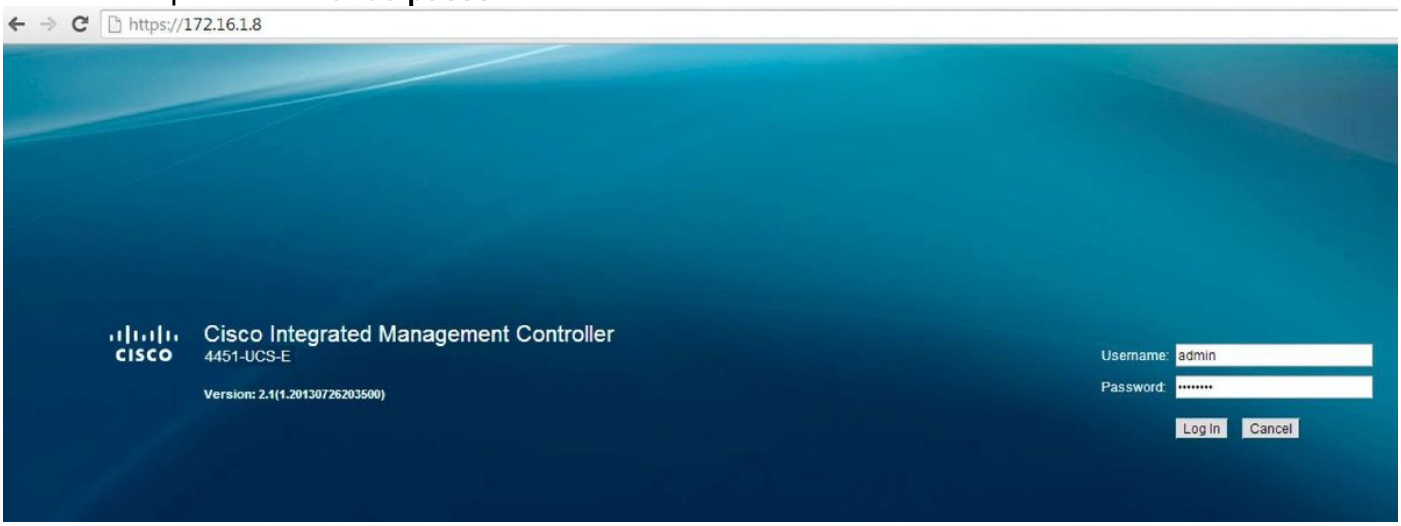
Exécutez la commande **show detail** afin de vérifier les paramètres de détail :

```
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 #
```

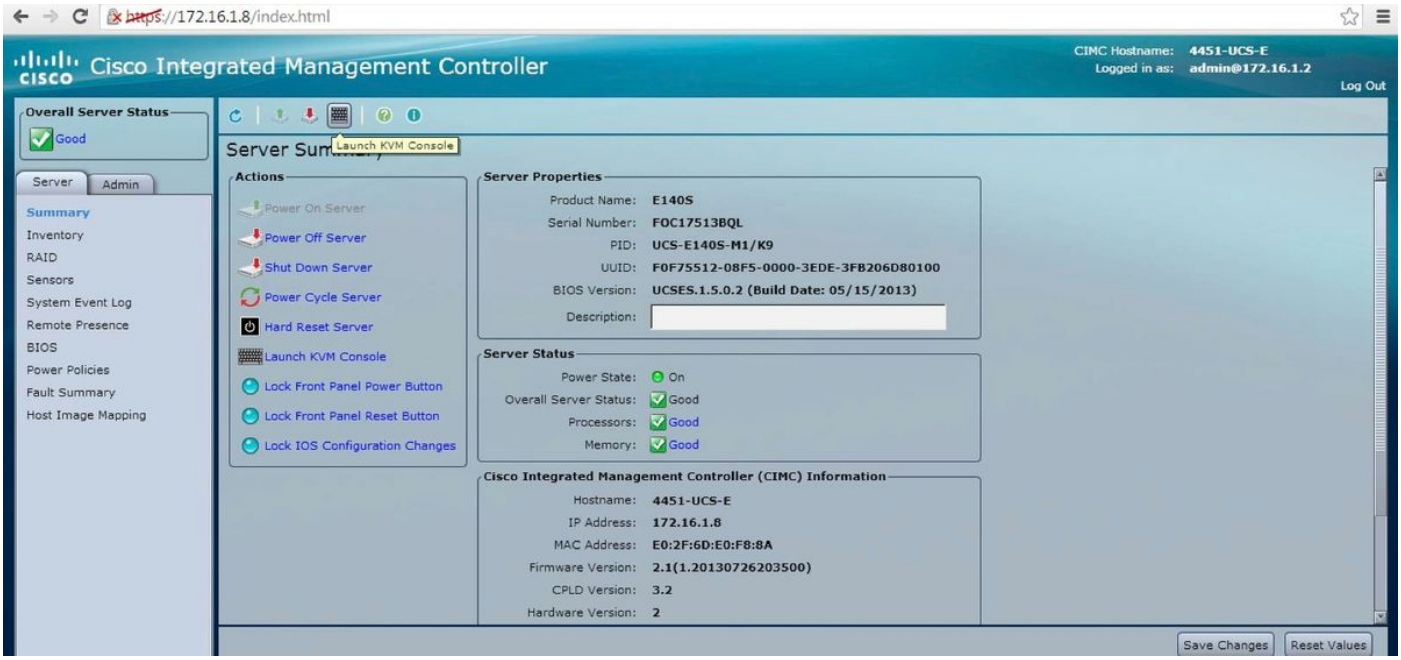
Lancez l'interface Web du CIMC à partir d'un navigateur avec le nom d'utilisateur et le mot de passe par défaut, comme indiqué dans l'image. Le nom d'utilisateur et le mot de passe par défaut sont les suivants :

- username (nom d'utilisateur) : **admin**
- Mot de passe : **<mot de passe>**

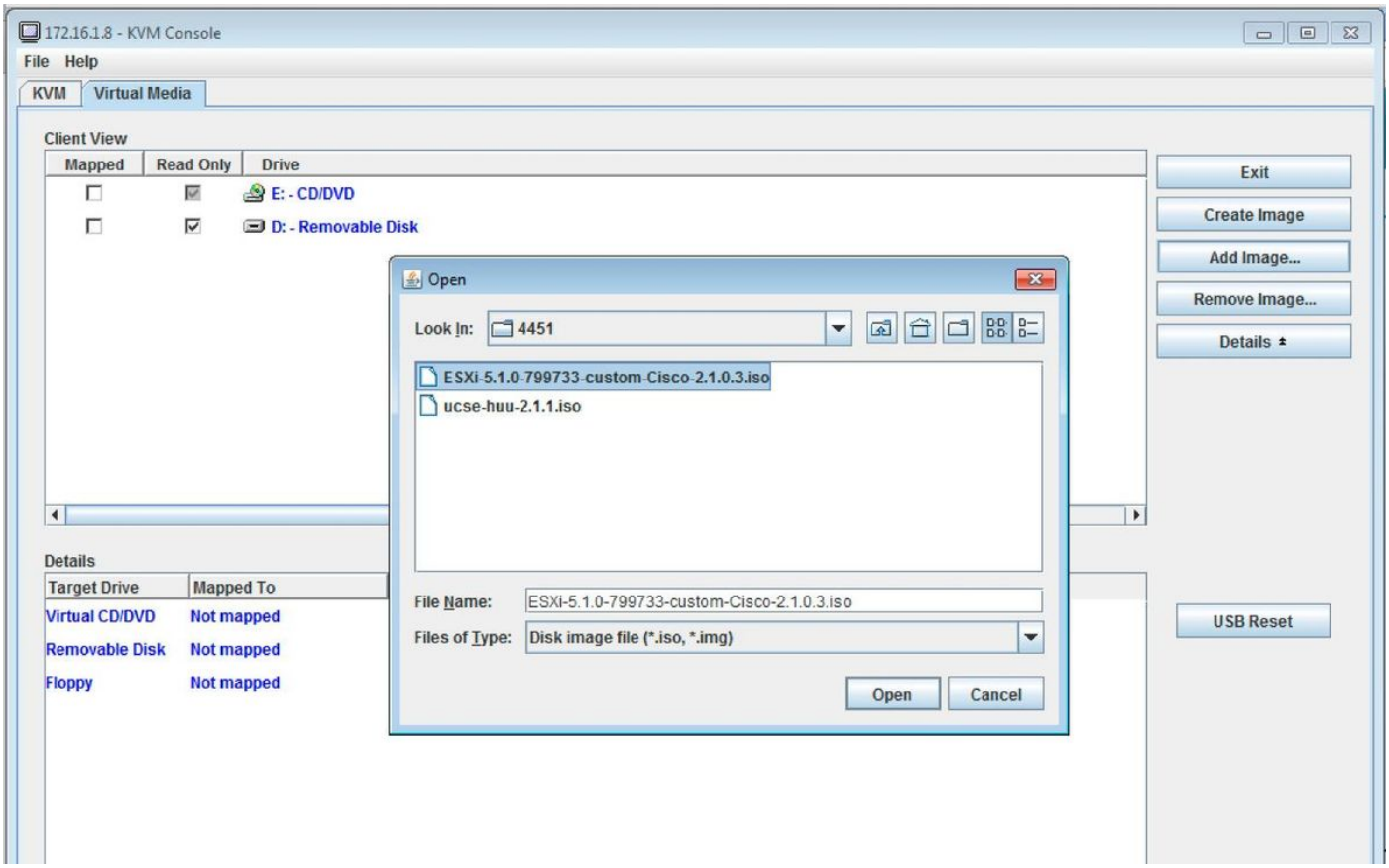


Installer ESXi

Après vous être connecté à l'interface utilisateur du CIMC, vous pouvez afficher une page similaire à celle illustrée dans cette image. Cliquez sur l'icône **Launch KVM Console**, cliquez sur **add image**, puis mappez l'ISO ESXi en tant que Virtual Media :



Cliquez sur l'onglet **Virtual Media**, puis cliquez sur **Ajouter une image** afin de mapper le média virtuel comme indiqué dans l'image.



Une fois le Virtual Media mappé, cliquez sur **Power Cycle Server** à partir de la page d'accueil CIMC afin de mettre sous tension le UCS-E. La configuration d'ESXi démarre à partir du Virtual Media. Terminez l'installation d'ESXi.

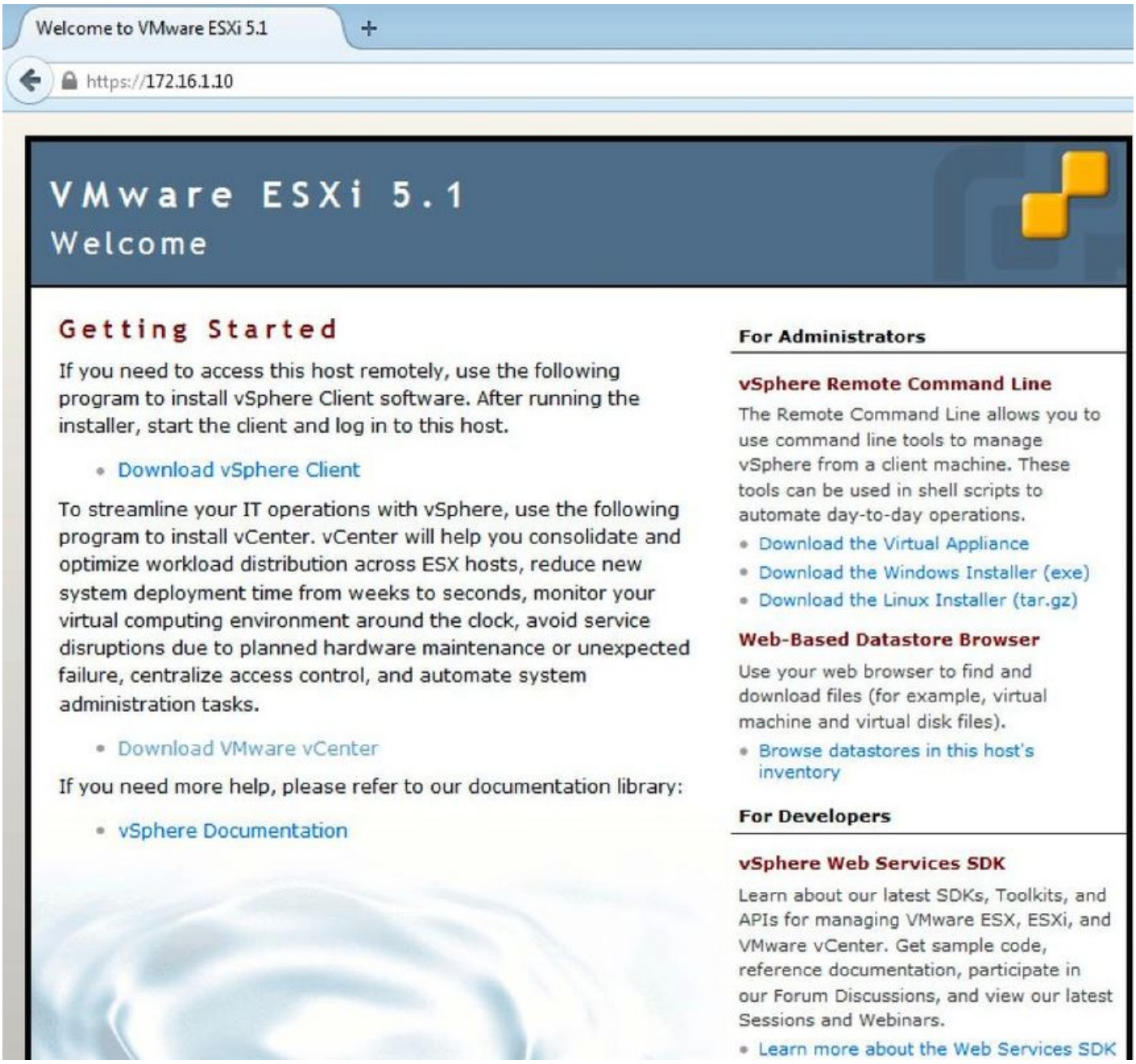
Note: Notez l'adresse IP, le nom d'utilisateur et le mot de passe ESXi pour référence future.

Installer le client vSphere

Cette section décrit comment installer le client vSphere.

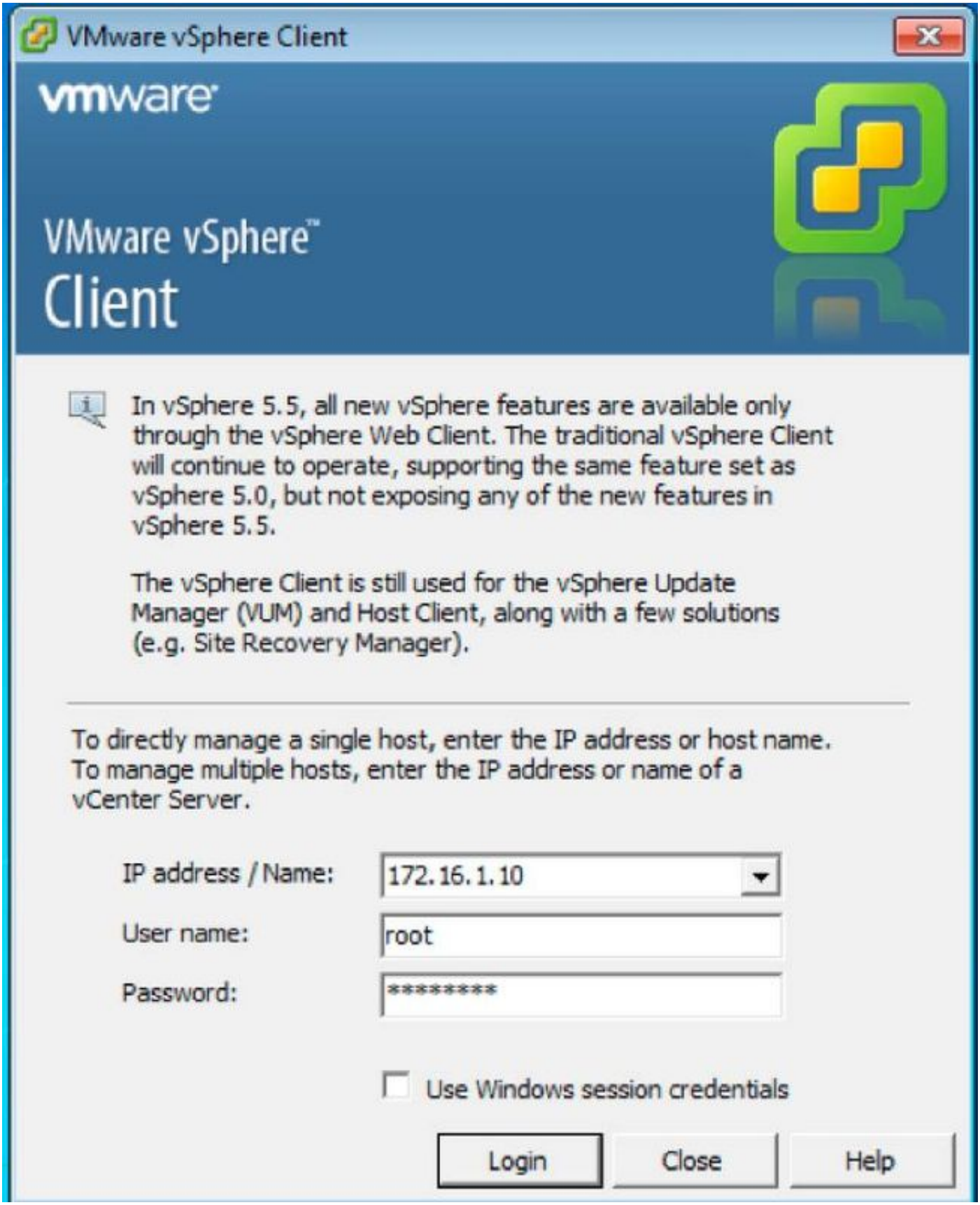
Télécharger le client vSphere

Lancez ESXi et utilisez le lien **Download VSphere Client** afin de télécharger le client vSphere. Installez-le sur votre ordinateur.



Lancer le client vSphere

Lancez le client vSphere à partir de votre ordinateur. Connectez-vous avec le nom d'utilisateur et le mot de passe que vous avez créés lors de l'installation, comme indiqué sur l'image :



Déployer FireSIGHT Management Center et les périphériques FirePOWER

Suivez les procédures décrites dans le document Deployment of FireSIGHT Management Center on VMware ESXi Cisco afin de déployer FireSIGHT Management Center sur ESXi.

Note: Le processus utilisé pour déployer un périphérique NGIPSv FirePOWER est similaire

au processus utilisé pour déployer un Management Center.

Interfaces

Sur le serveur UCS-E double largeur, il existe quatre interfaces :

- L'interface d'adresse MAC la plus élevée est Gi3 sur la façade.
- La deuxième interface d’adresse MAC la plus élevée est Gi2 sur la façade
- Les deux dernières qui apparaissent sont des interfaces internes

Sur le serveur UCS-E simple largeur, il existe trois interfaces :

- L'interface d'adresse MAC la plus élevée est Gi2 sur la façade.
- Les deux dernières qui apparaissent sont des interfaces internes

Les deux interfaces UCS-E du routeur ISR4K sont des ports agrégés.

Les serveurs UCS-E 120S et 140S disposent de trois adaptateurs réseau et de trois ports de gestion :

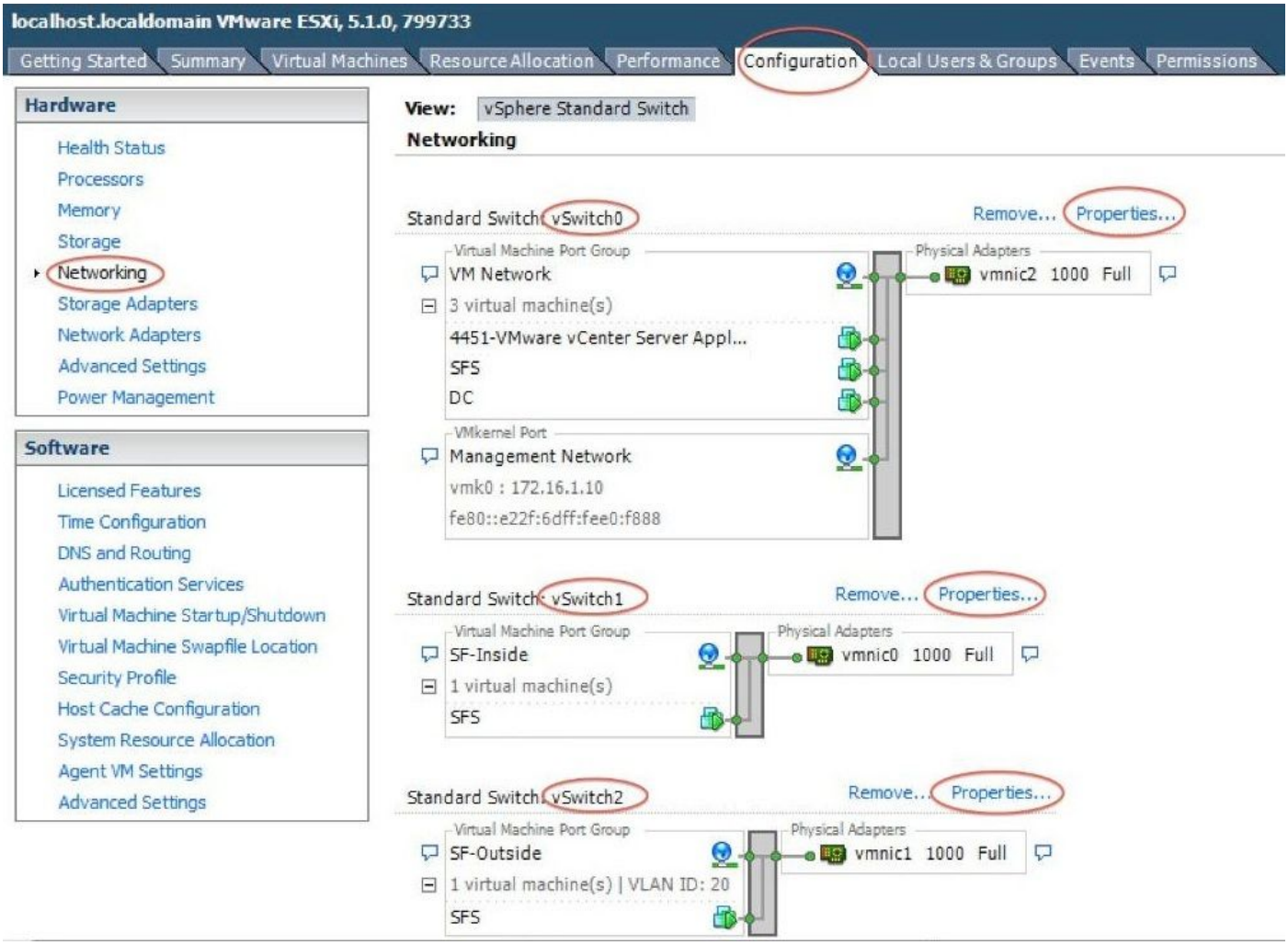
- Le *vmnic0* est mappé à *UCSEx/0/0* sur le fond de panier du routeur
- Le *vmnic1* est mappé à *UCSEx/0/1* sur le fond de panier du routeur
- Le *vmnic2* est mappé à l'interface GE2 du plan avant UCS-E
- Le port de gestion du panneau avant (M) ne peut être utilisé que pour le CIMC.

Les serveurs UCS-E 140D, 160D et 180D disposent de quatre adaptateurs réseau :

- Le *vmnic0* est mappé à *UCSEx/0/0* sur le fond de panier du routeur.
- Le *vmnic1* est mappé à *UCSEx/0/1* sur le fond de panier du routeur.
- Le *vmnic2* est mappé à l'interface GE2 du plan avant UCS-E.
- Le *vminc3* est mappé à l'interface GE3 du plan avant UCS-E.
- Le port de gestion du panneau avant (M) ne peut être utilisé que pour le CIMC.

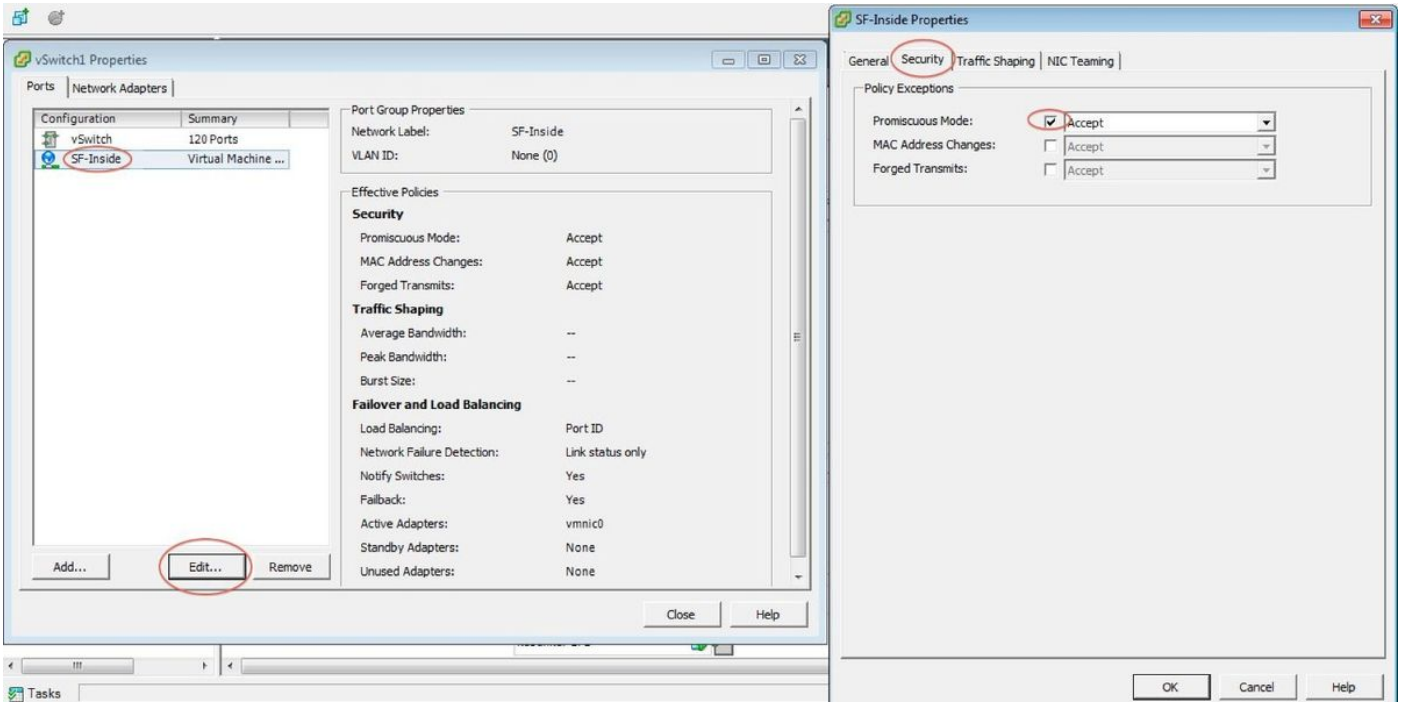
Interfaces vSwitch sur ESXi

Le vSwitch0 de l'ESXi est l'interface de gestion par laquelle ESXi, FireSIGHT Management Center et le périphérique NGIPSv FirePOWER communiquent avec le réseau. Cliquez sur **Properties** pour vSwitch1 (SF-Inside) et vSwitch2 (SF-Outside) afin d'apporter des modifications.



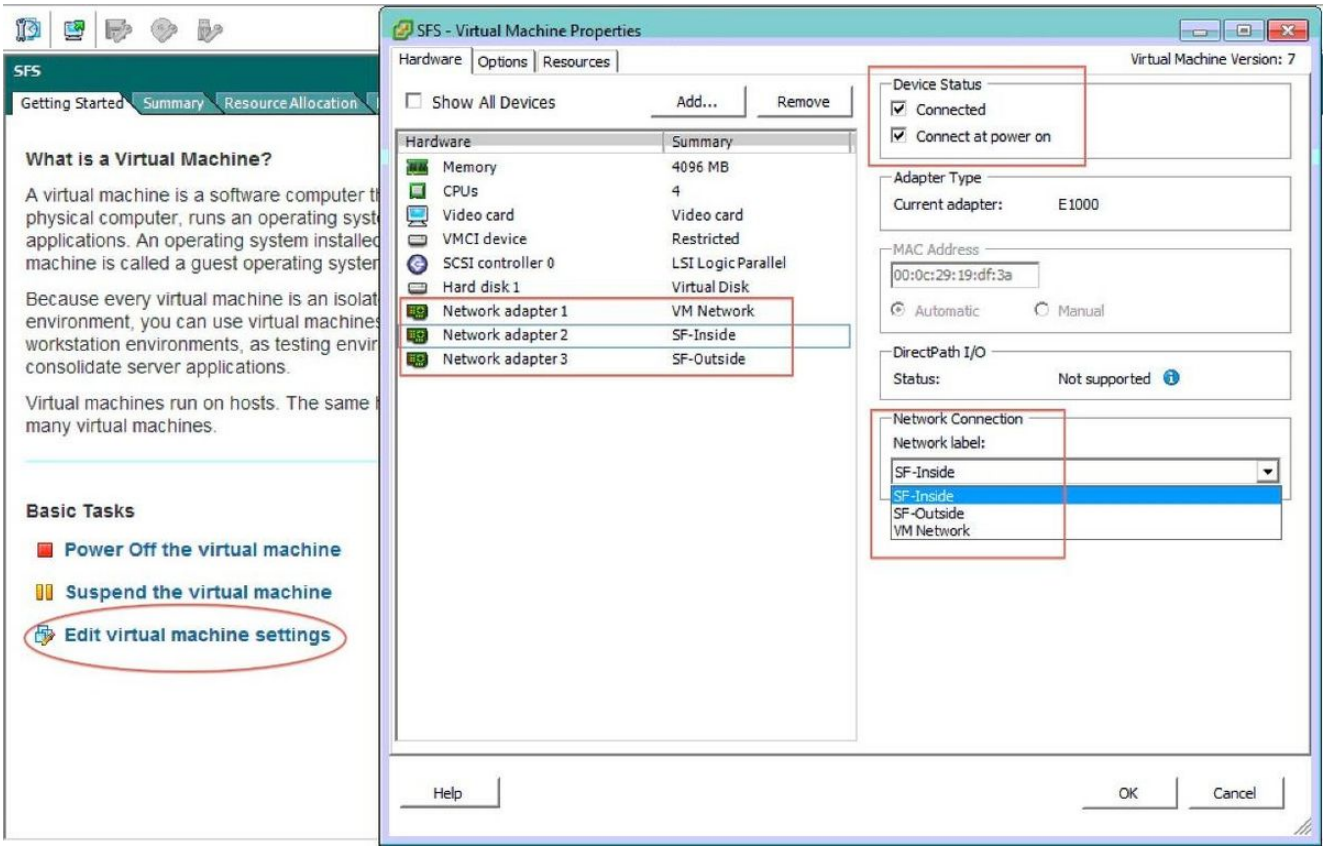
Cette image montre les propriétés du vSwitch1 (vous devez effectuer les mêmes étapes pour le vSwitch2) :

> **Note**: Assurez-vous que l'ID de VLAN est configuré sur 4095 pour NGIPSv, ceci est requis conformément au document NGIPSv : http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



La configuration du commutateur virtuel sur l'ESXi est terminée. Vous devez maintenant vérifier les paramètres d'interface :

1. Accédez à la machine virtuelle du périphérique FirePOWER.
2. Cliquez sur **Modifier les paramètres de la machine virtuelle**.
3. Vérifiez les trois cartes réseau.
4. Assurez-vous qu'ils sont correctement choisis, comme le montre l'image ici :



Enregistrez le périphérique FirePOWER avec FireSIGHT Management Center

Suivez les procédures décrites dans le document Cisco afin d'enregistrer un périphérique FirePOWER avec FireSIGHT Management Center.

Rediriger et vérifier le trafic

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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

Rediriger le trafic de l'ISR vers le capteur sur UCS-E

Utilisez ces informations afin de rediriger 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 ultérieure, exécutez la commande **utd engine advanced** au lieu de la commande **utd**.

Vérification de la redirection de paquet

Àpartir de la console ISR, exécutez cette commande afin de vérifier si les compteurs de paquets s'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
```

Vérification

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

- **show plat software utd global**
- **show plate software utd interfaces**
- **show plat software utd rp active global**
- **show plat software utp fp active global**
- **show plat hardware qfp active feature utd stats**
- **show platform hardware qfp active feature utd**

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Vous pouvez exécuter ces commandes **debug** afin de dépanner votre configuration :

- **debug platform condition feature utd controlplane**
- **debug platform condition feature utd'utd dataplane submode**

Informations connexes

- Guide de démarrage pour les serveurs Cisco UCS E et le moteur de calcul réseau Cisco UCS E, version 2.x
- Guide de dépannage des serveurs Cisco UCS E et du moteur de calcul réseau Cisco UCS E
- Guide de démarrage pour les serveurs Cisco UCS E et Cisco UCS E-Series Network Compute Engine, version 2.x - Mise à niveau du micrologiciel
- Guide de configuration du logiciel des routeurs à services d'agrégation de la gamme Cisco ASR 1000 - Configuration des interfaces de domaine de pont
- Guide d'utilisation de l'utilitaire de mise à niveau d'hôte pour les serveurs Cisco UCS E et le moteur de calcul réseau Cisco UCS E - Mise à niveau du micrologiciel sur les serveurs Cisco UCS E
- Support et documentation techniques - Cisco Systems