使用UCS-E刀片在ISR裝置上配置FirePOWER服務

目錄

簡介

本檔案介紹如何在入侵偵測系統(IDS)模式下在Cisco Unified Computing System E系列(UCS-E)刀鋒平台上安裝和部署Cisco FirePOWER軟體。本文檔中介紹的配置示例是對官方使用手冊的補充。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Integrated Services Routers(ISR)XE image 3.14或更高版本
- 思科整合式管理控制器(CIMC)版本2.3或更新版本
- Cisco FireSIGHT管理中心(FMC)版本5.2或更高版本
- Cisco FirePOWER虛擬裝置(NGIPSv)版本5.2或更高版本
- VMware ESXi版本5.0或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

> **附註**：在將代碼升級到版本3.14或更高版本之前，請確保系統具有足夠的記憶體、磁碟空間以及升級許可證。請參閱範例1:將映像複製到flash:從TFTP伺服器部分，從Access Routers軟體升級過程思科文檔瞭解更多有關代碼升級的資訊。

> **附註**：要升級CIMC、BIOS和其他韌體元件，您可以使用Cisco Host Upgrade Utility(HUU)，也可以手動升級韌體元件。要瞭解有關韌體升級的詳細資訊，請參閱Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎的主機升級實用程式使用手冊的在Cisco UCS E系列伺服器上升級韌體部分。

背景資訊

本節介紹與本文檔中介紹的元件和過程相關的支援的硬體平台、許可證和限制的相關資訊。

支援的硬體平台

本部分列出了G2和4000系列裝置支援的硬體平台。

採用UCS-E刀片的ISR G2裝置

支援以下具有UCS-E系列刀片的ISR G2系列裝置：

產品	平台	UCS-E型號
Cisco 2900系列ISR	2911	UCS-E 120/140單寬選件
	2921	UCS-E 120/140/160/180單寬或雙寬選項
	2951	UCS-E 120/140/160單寬或雙寬選項
Cisco 3900系列ISR	3925	UCS-E 120/140/160單寬和雙寬選項或180雙寬
	3925E	UCS-E 120/140/160單寬和雙寬選項或180雙寬
	3945	UCS-E 120/140/160單寬和雙寬選項或180雙寬
	3945E	UCS-E 120/140/160單寬和雙寬選項或180雙寬

採用UCS-E刀片的ISR 4000裝置

支援以下具有UCS-E系列刀片的ISR 4000系列裝置：

產品	平台 UCS-E型號
Cisco 4400系列ISR	4451 UCS-E 120/140/160單寬和雙寬選項或180雙寬 4431 UCS-E網路介面模組
Cisco 4300系列ISR	4351 UCS-E 120/140/160/180單寬和雙寬選項或180雙寬 4331 UCS-E 120/140單寬選件 4321 UCS-E網路介面模組

授權

ISR必須具有安全K9許可證以及appx許可證，才能啟用該服務。

限制

以下為與本檔案所述資訊有關的兩個限制：

- 不支援組播
- 每個系統僅支援4,096個網橋域介面(BDI)

BDI不支援以下功能：

- 雙向轉發檢測(BFD)協定
- Netflow
- 服務品質(QoS)
- 網路型應用程式辨識(NBAR)或進階視訊編碼(AVC)
- 區域型防火牆(ZBF)
- 加密VPN
- 多重協定標籤交換 (MPLS)
- 乙太網路上的點對點通訊協定(PPP)(PPPoE)

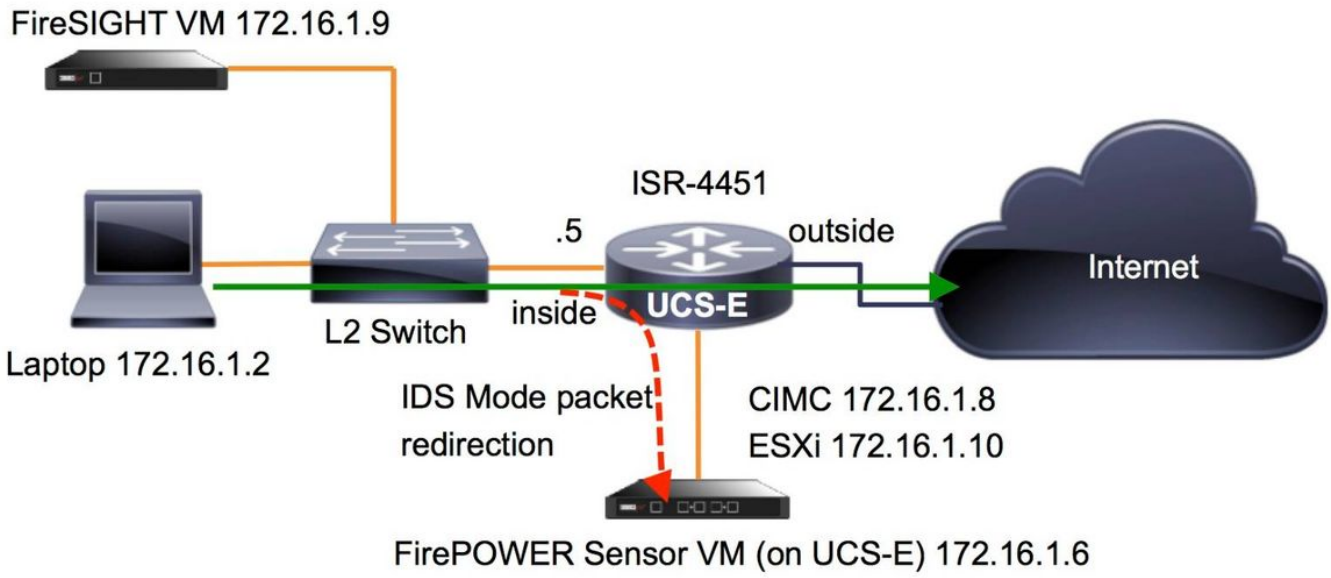
附註：對於BDI，最大傳輸單元(MTU)大小可配置為1,500到9,216位元組之間的任何值。

設定

本節介紹如何配置與此部署相關的元件。

網路圖表

本檔案所述的組態使用以下網路拓撲：



UCS-E上FirePOWER服務的工作流程

以下是在UCS-E上運行的FirePOWER服務的工作流程：

1. 資料平面將流量從BDI/UCS-E介面推出以進行檢查（適用於G2和G3系列裝置）。
2. Cisco IOS®-XE CLI啟用資料包重定向進行分析（所有介面或每個介面的選項）。
3. 感測器CLI設置啟動指令碼簡化了配置。

配置CIMC

本節介紹如何配置CIMC。

連線到CIMC

連線到CIMC的方法有多種。在本示例中，通過專用管理埠完成與CIMC的連線。確保使用乙太網電纜將M埠（專用）連線到網路。連線後，在路由器提示符下運行**hw-module subslot**命令：

```
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
```

提示1:要退出，請運行**^a^q**。

提示2:預設使用者名稱是**admin**，密碼為<password>。密碼重置過程如下所述：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

配置CIMC

使用以下資訊完成CIMC的配置：

```
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
```

注意：確保運行**commit**命令以儲存更改。

附註：使用管理埠時，模式設定為**dedicated**。

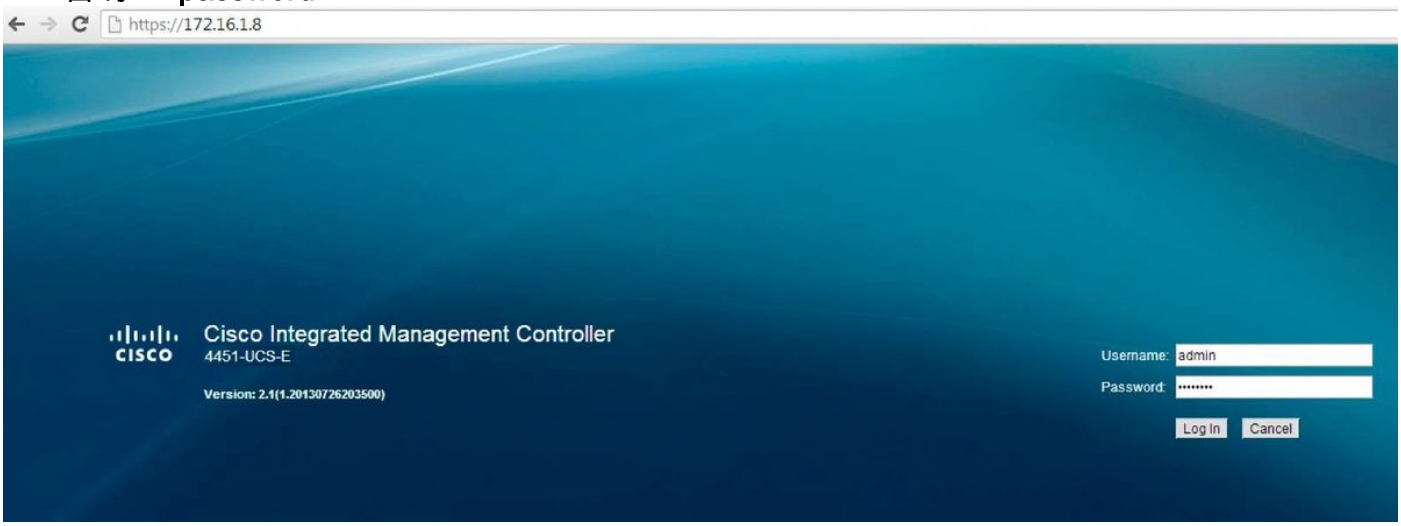
執行**show detail**命令以驗證詳細資訊設定：

```
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 #
```

使用預設使用者名稱和密碼從瀏覽器啟動CIMC的Web介面，如下圖所示。預設使用者名稱和密碼為：

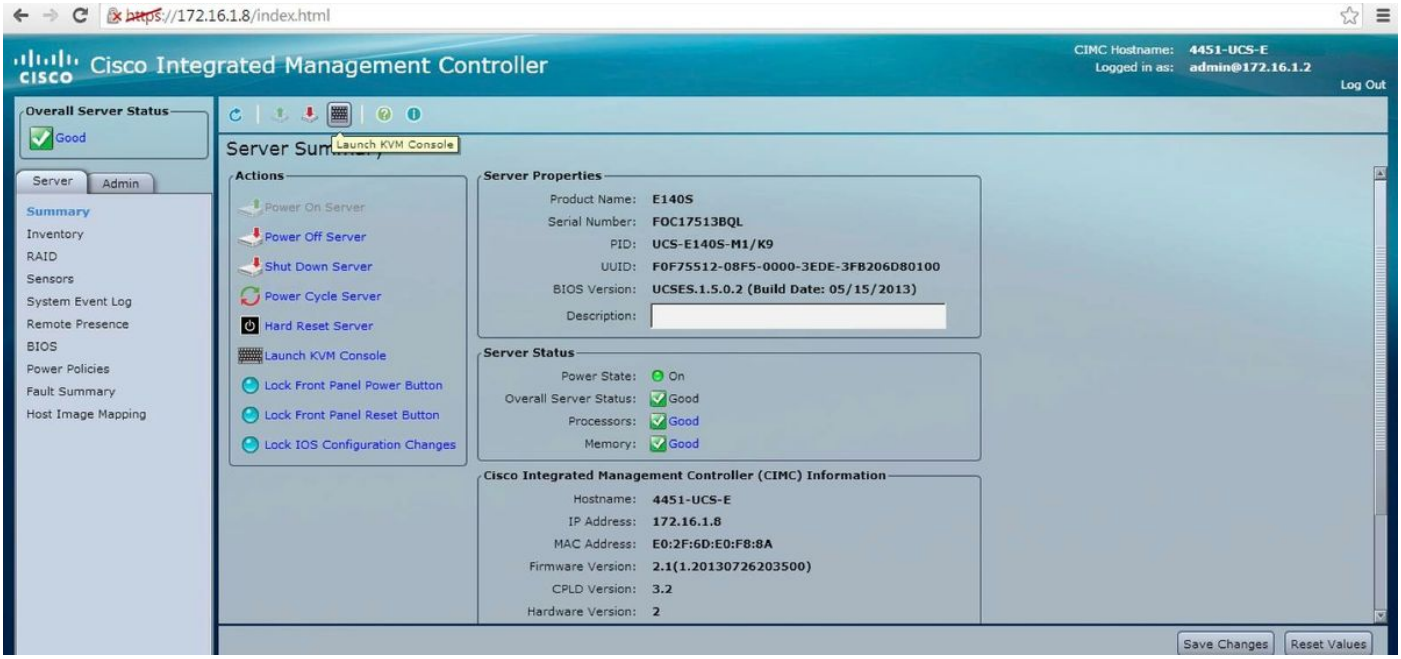
- 使用者名稱:**admin**

- 密碼：<password>

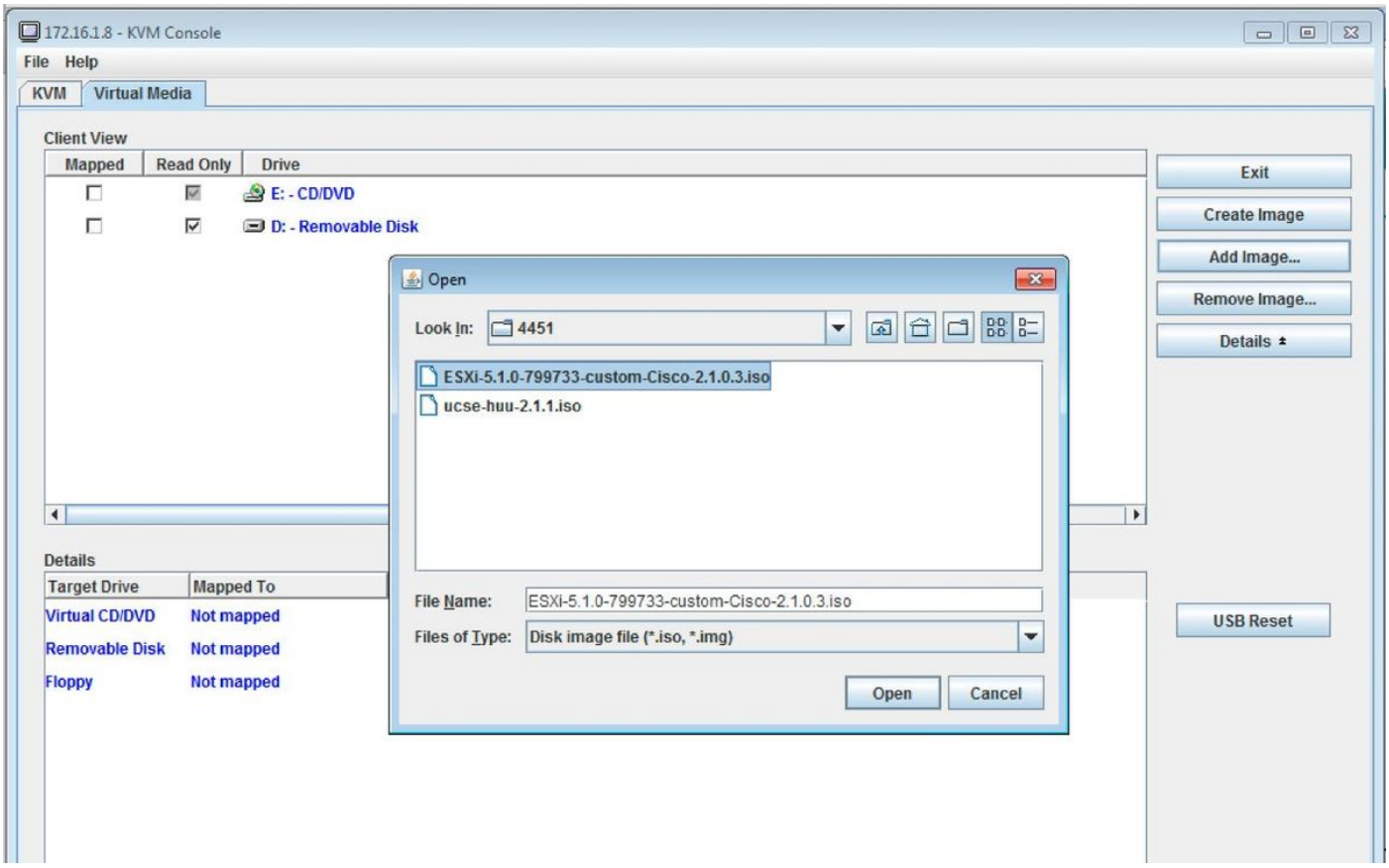


安裝ESXi

登入到CIMC的使用者介面後，您可以檢視與下圖所示類似的頁面。按一下**Launch KVM Console**圖示，按一下**add image**，然後將ESXi ISO對映為虛擬介質：



按一下**Virtual Media**頁籤，然後按一下**Add Image**以對映虛擬媒體，如圖所示。



對映虛擬介質後，從CIMC首頁點選**Power Cycle Server**以重新啟動UCS-E。ESXi安裝程式從虛擬介質啟動。完成ESXi安裝。

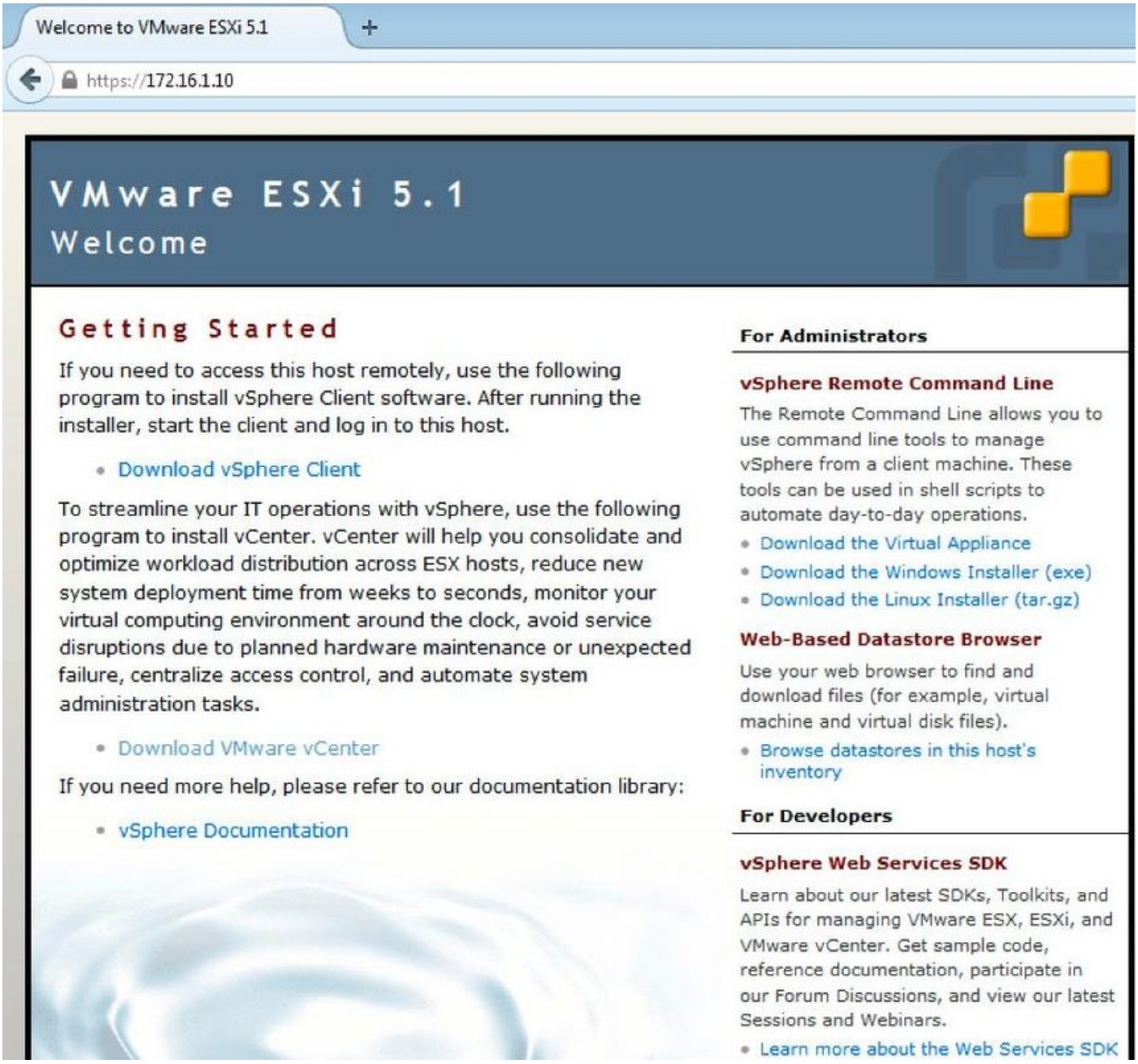
附註：記錄ESXi IP地址、使用者名稱和密碼以供將來參考。

安裝vSphere客戶端

本節介紹如何安裝vSphere客戶端。

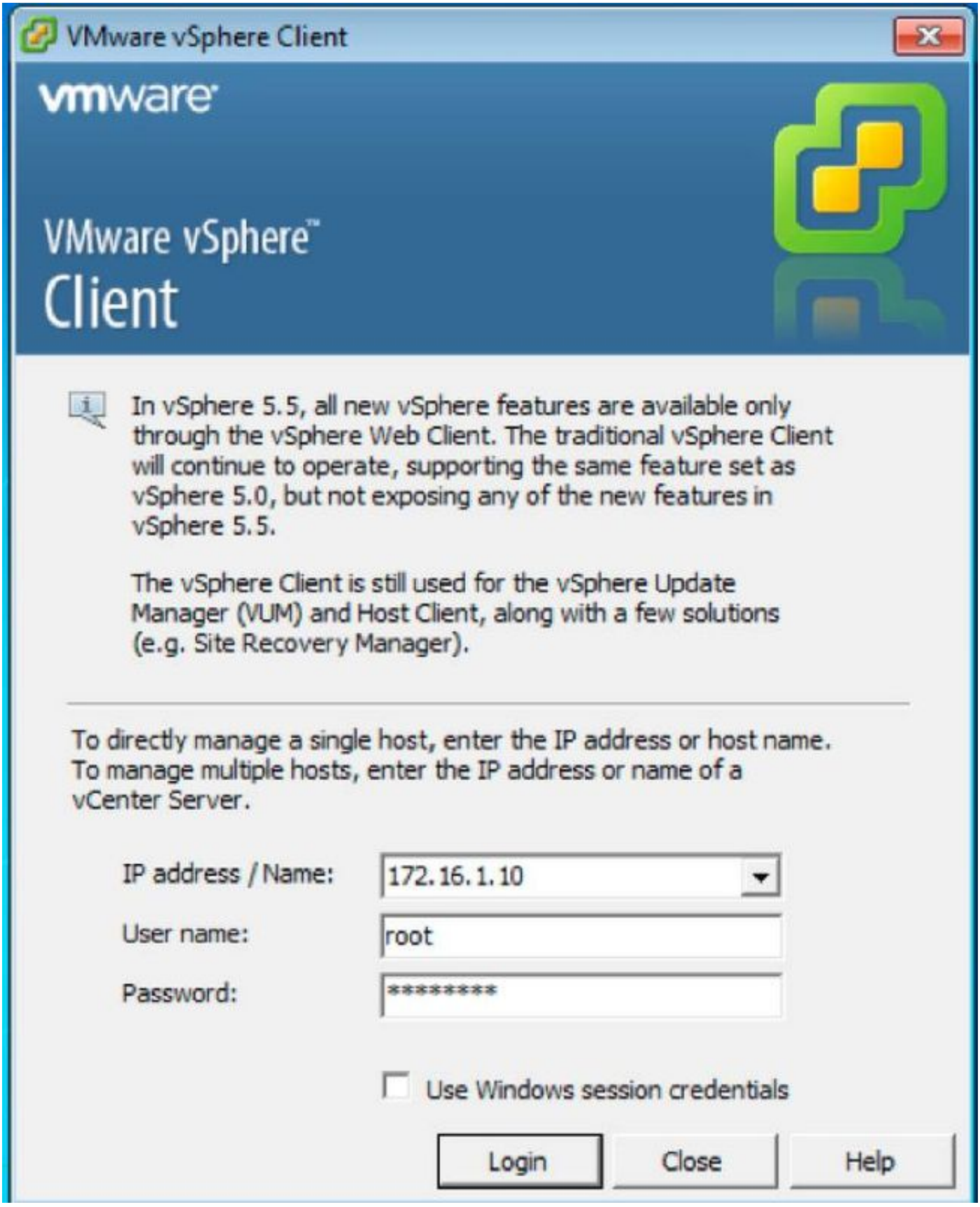
下載vSphere客戶端

啟動ESXi並使用**Download VSphere Client**連結下載vSphere客戶端。將其安裝在電腦上。



啟動vSphere客戶端

從電腦啟動vSphere客戶端。使用您在安裝期間建立的使用者名稱和密碼登入，如下圖所示：



部署FireSIGHT管理中心和FirePOWER裝置

完成在VMware ESXi思科上部署FireSIGHT管理中心文檔中所述的步驟，以便在ESXi上部署FireSIGHT管理中心。

附註：用於部署FirePOWER NGIPSv裝置的過程與用於部署管理中心的過程類似。

介面

在雙寬UCS-E上，有四個介面：

- 最大MAC地址介面是前面板上的Gi3
- 第二高MAC地址介面是前面板上的Gi2
- 顯示的最後兩個是內部介面

在單寬UCS-E上，有三個介面：

- 最大的MAC地址介面是前面板上的Gi2
- 顯示的最後兩個是內部介面

ISR4K上的兩個UCS-E介面都是中繼埠。

UCS-E 120S和140S有三個網路介面卡和管理埠：

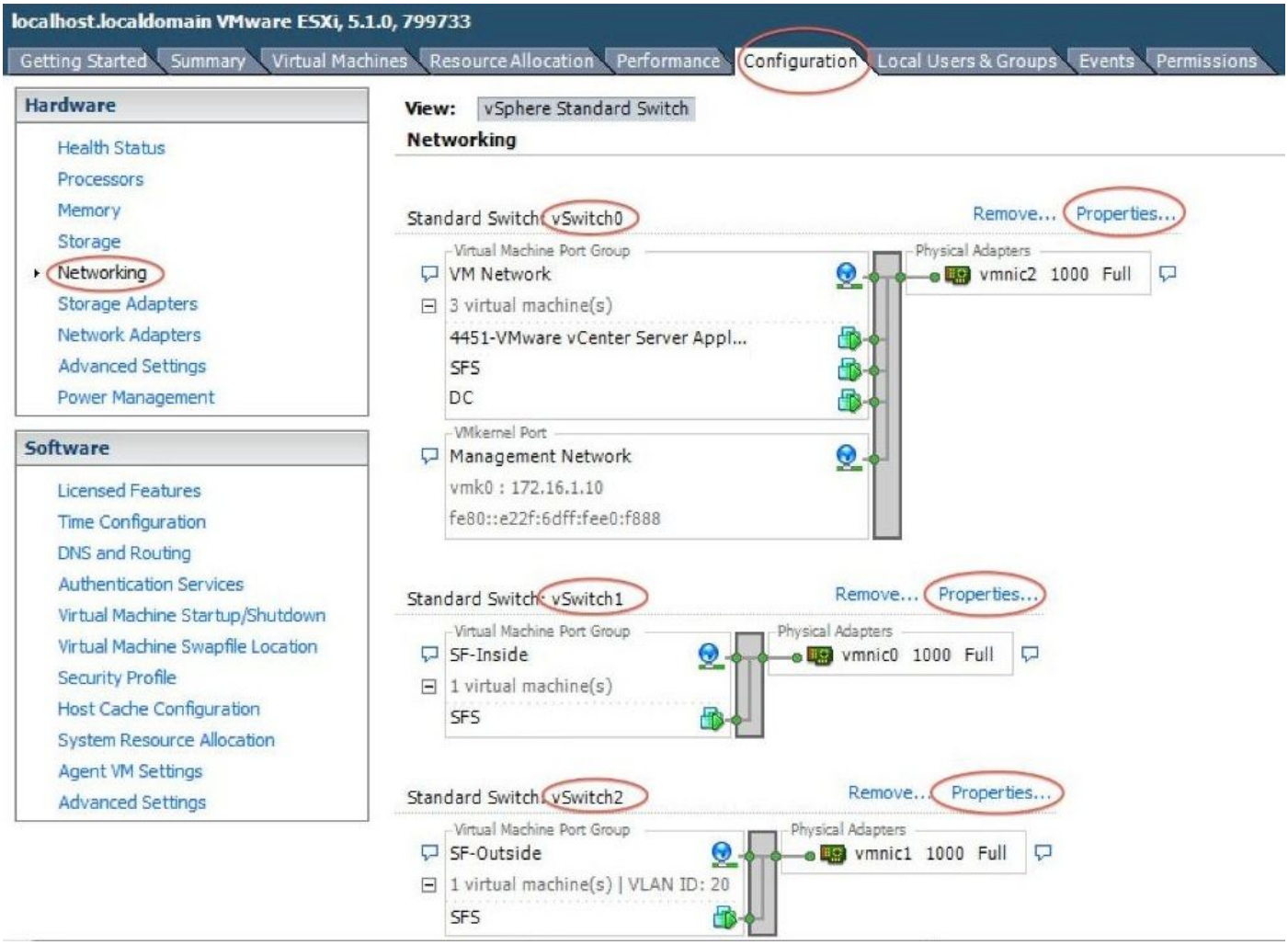
- *vmnic0*對映到路由器背板上的*UCSEx/0/0*
- *vmnic1*對映到路由器背板上的*UCSEx/0/1*
- *vmnic2*對映到UCS-E前平面GE2介面
- 前面板管理(M)埠只能用於CIMC。

UCS-E 140D、160D和180D具有四個網路介面卡：

- *vmnic0*對映到路由器背板上的*UCSEx/0/0*。
- *vmnic1*對映到路由器背板上的*UCSEx/0/1*。
- *vmnic2*對映到UCS-E前平面GE2介面。
- *vminc3*對映到UCS-E前平面GE3介面。
- 前面板管理(M)埠只能用於CIMC。

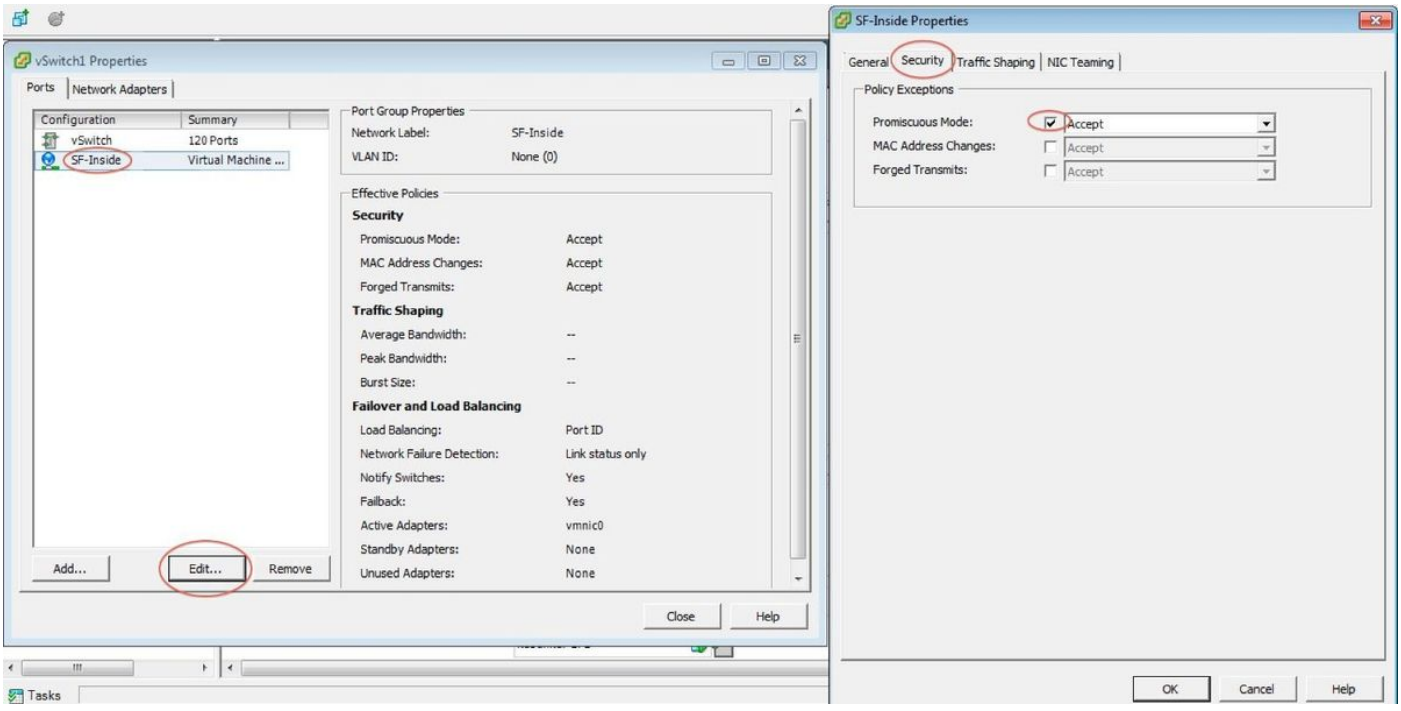
ESXi上的vSwitch介面

ESXi上的vSwitch0是ESXi、FireSIGHT管理中心和FirePOWER NGIPSv裝置通過網路通訊的管理介面。按一下vSwitch1(SF-Inside)和vSwitch2(SF-Outside)的**Properties**以進行更改。



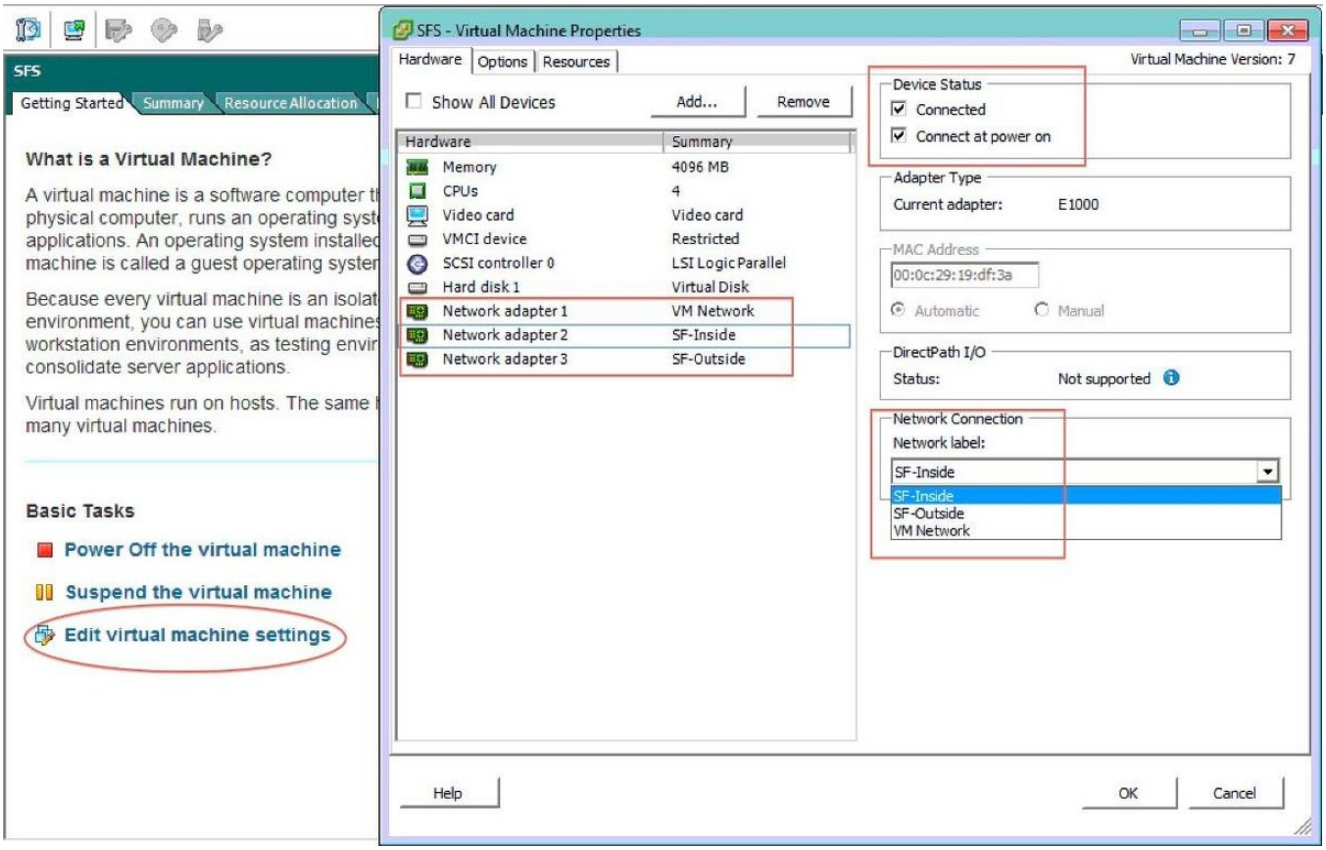
此圖顯示vSwitch1的屬性（您必須為vSwitch2完成相同的步驟）：

附註：確保將NGIPSv的VLAN ID配置為4095，根據NGIPSv文檔，這是必需的：http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



ESXi上的vSwitch配置已完成。現在，您必須驗證介面設定：

1. 導航到FirePOWER裝置的虛擬機器。
2. 按一下**Edit virtual machine settings**。
3. 檢驗所有三個網路介面卡。
4. 確保正確選擇它們，如下圖所示：



向FireSIGHT管理中心註冊FirePOWER裝置

完成思科文檔中所述的程式，以便向FireSIGHT管理中心註冊FirePOWER裝置。

重新導向和驗證流量

使用本節內容，確認您的組態是否正常運作。

本節介紹如何重新導向流量以及如何驗證封包。

將通訊量從ISR重定向到UCS-E上的感測器

使用以下資訊重新導向流量：

```
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
```

> **附註**：如果當前運行的是3.16.1版或更高版本，請運行**utd engine advanced**命令，而不是**utd**命令。

驗證封包重新導向

在ISR控制檯中運行此命令，以驗證資料包計數器是否增加：

```
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
```

驗證

您可以執行以下**show**命令以驗證您的組態是否正常運作：

- **show platt software utd global**
- **show platt software utd interfaces**
- **show platt software utd rp active global**
- **show platt software utd fp active global**
- **show platt hardware qfp active feature utd stats**
- **show platform hardware qfp active feature utd**

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

您可以運行以下**debug**命令對組態進行疑難排解：

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

相關資訊

- Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎入門指南2.x版
- Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎故障排除指南
- Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎入門指南2.x版 — 升級韌體
- Cisco ASR 1000系列聚合服務路由器軟體配置指南 — 配置網橋域介面
- Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎的主機升級實用程式使用手冊 — 升級Cisco UCS E系列伺服器上的韌體
- 技術支援與文件 - Cisco Systems