# UCS-E ブレード付き ISR デバイス上で FirePOWER サービスを設定する

## 目次



## 概要

このドキュメントでは、Instusion Detection System（IDS）モードで Cisco Unified Computing System E Series（UCS-E）ブレード プラットフォーム上に Cisco FirePOWER ソフトウェアをインストールし、展開する方法について説明します。 このドキュメントで説明している設定の例は、正式なユーザ ガイドを補足するものです。

# 前提条件

## 要件

このドキュメントに関しては個別の要件はありません。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Integrated Services Routers（ISR）XE image 3.14 以降
- Cisco Integrated Management Controller（CIMC）バージョン 2.3 以降
- Cisco FireSIGHT Management Center（FMC）バージョン 5.2 以降
- Cisco FirePOWER Virtual Device（NGIPSv）バージョン 5.2 以降
- VMware ESXi バージョン 5.0 以降

  **注:** コードをバージョン 3.14 以降にアップグレードする前に、アップグレード用の十分なメモリ、ディスク領域、ライセンスがシステムにあることを確認します。「例 1： TFTP サーバから flash: へイメージを コピー」のセクション（Cisco ドキュメント『*アクセス ルータ ソフトウェアのアップグレード手順*』）を参照して、コードのアップグレードの詳細情報を確認してください。

  CIMC、BIOS、その他のファームウェア コンポーネントをアップグレードするには、Cisco Host Upgrade Utility（HUU）を使用するか、ファームウェア コンポーネントを手動でアップグレードできます。 ファームウェア アップグレードの詳細については、『*Host Upgrade Utility User Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*』の「Cisco UCS E-Series Servers でのファームウェア アップグレード」のセクションを参照してください。

# 背景説明

このセクションでは、このドキュメントで説明するコンポーネントと手順に関連してサポートされるハードウェア プラットフォーム、ライセンス、および制限事項の情報を提供します。

## サポートされているハードウェア プラットフォーム

ここでは、G2 および 4000 シリーズ デバイスでサポートされるハードウェア プラットフォームを記載しています。

### UCS-E ブレードを搭載した ISR G2 デバイス

UCS-E ブレードを搭載したこれらの ISR G2 デバイスがサポートされます：

| 製品 | プラットフォーム UCS-E モデル |
|---|---|

| | | |
|---|---|---|
| Cisco 2900 シリーズ ISR | 2911 | UCS-E 120/140 シングル幅オプション |
| | 2921 | UCS-E 120/140/160/180 シングル幅またはダブル幅オプション |
| | 2951 | UCS-E 120/140/160 シングル幅またはダブル幅オプション |
| Cisco 3900 シリーズ ISR | 3925 | UCS-E 120/140/160 シングル幅およびダブル幅オプション、ま 180 ダブル幅 |
| | 3925E | UCS-E 120/140/160 シングル幅およびダブル幅オプション、ま 180 ダブル幅 |
| | 3945 | UCS-E 120/140/160 シングル幅およびダブル幅オプション、ま 180 ダブル幅 |
| | 3945E | UCS-E 120/140/160 シングル幅およびダブル幅オプション、ま 180 ダブル幅 |

### UCS-E ブレードを搭載した ISR 4000 デバイス

UCS-E ブレードを搭載したこれらの ISR 4000 デバイスがサポートされます：

| 製品 | プラットフォーム | UCS-E モデル |
|---|---|---|
| Cisco 4400 シリーズ ISR | 4451 | UCS-E 120/140/160 シングル幅およびダブル幅オプション、ま 180 ダブル幅 |
| | 4431 | UCS-E ネットワーク インターフェイス モジュール |
| Cisco 4300 シリーズ ISR | 4351 | UCS-E 120/140/160/180 シングル幅およびダブル幅オプション、 たは 180 ダブル幅 |
| | 4331 | UCS-E 120/140 シングル幅オプション |
| | 4321 | UCS-E ネットワーク インターフェイス モジュール |

## ライセンス

サービスを有効にするには、ISR で *appx* ライセンスおよびセキュリティ K9 ライセンスが必要です。

## 制限事項

このドキュメントで説明している内容について、2 つの制限事項があります：

- マルチキャストはサポートされません。
- システムごとにサポートされるブリッジ ドメイン インターフェイス（BDI）は 4,096 個のみです。

BDI では、次の機能をサポートしていません。

- 双方向フォワーディング検出（BFD）プロトコル
- NetFlow
- Quality of Service（QoS）
- Network-Based Application Recognition（NBAR）または Advanced Video Coding（AVC）
- ゾーンベース ファイアウォール（ZBF）

- 暗号化 VPN
- マルチプロトコル ラベル スイッチング（MPLS）
- Point-to-Point Protocol（PPP）over Ethernet（PPPoE）

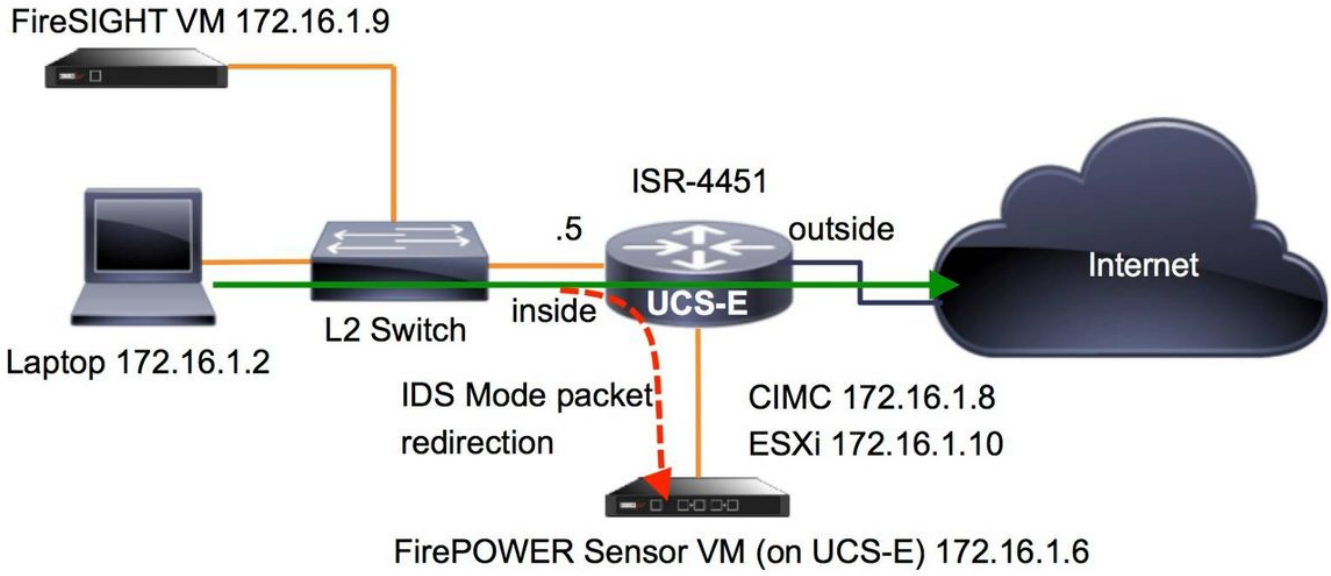
  **注:** BDI の場合、最大伝送ユニット（MTU）サイズを 1,500 ~ 9,216 バイトの間の任意の値で設定できます。

# 設定

このセクションでは、この実装に含まれるコンポーネントを設定する方法について説明します。

## ネットワーク図

このドキュメントで説明する設定では、このネットワーク トポロジを使用します：




## UCS-E 上の FirePOWER サービスのワークフロー

UCS-E で実行される FirePOWER サービスのワークフローを次に示します。

1. データプレーンは BDI/UCS-E インターフェイス（G2 および G3 シリーズ デバイスで動作）から検査用のトラフィックをプッシュします。
2. Cisco IOS-XE CLI が分析用にパケット リダイレクションを有効化します（すべてのインターフェイスまたはインターフェイス別のオプション）。
3. センサー CLI の *setup* 起動スクリプトにより、簡単に設定できます。

## CIMC の設定

ここでは、CIMC を設定する方法について説明します。

## CIMC への接続

CIMC に接続するには複数の方法があります。 この例では、専用の管理ポートを介して CIMC に接続します。 イーサネット ケーブルを使用して、M ポート（専用）をネットワークに接続していることを確認します。 接続されたら、ルータ プロンプトから hw-module subslot コマンドを入力します：

```
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
```

**ヒント**： 終了するには ^a^q と入力します。

## CIMC の設定

CIMC の設定を完了するには、次の情報を使用します。

```
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**： 変更を保存するには commit コマンドを必ず入力してください。

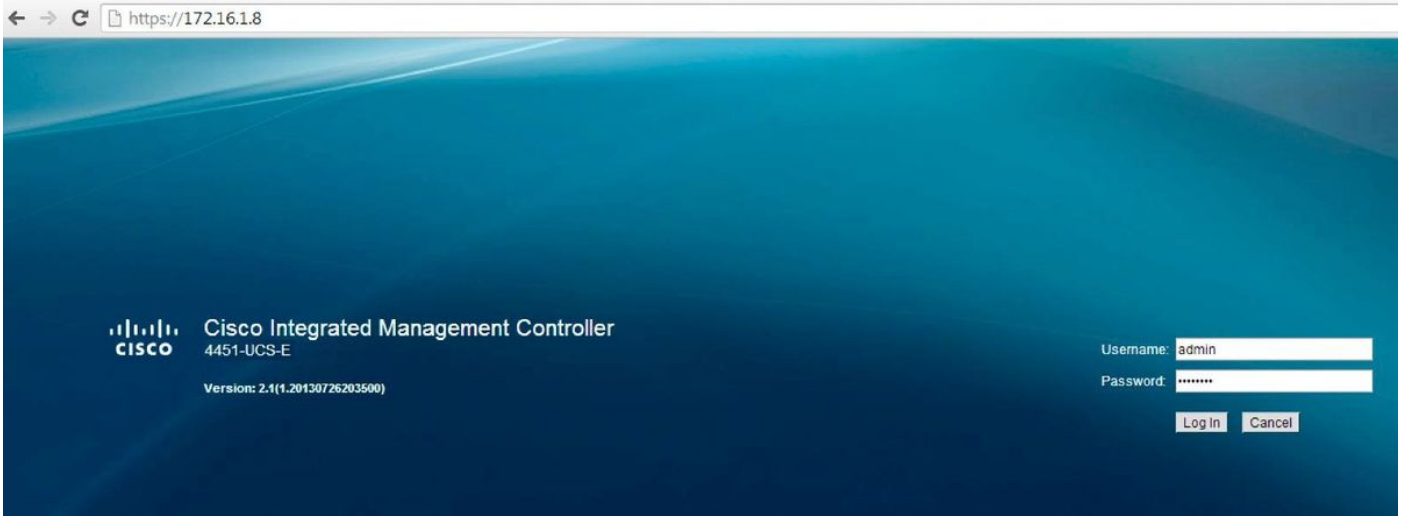
**注:** 管理ポートを使用するときには、*モード*が [dedicated]（専用）に設定されます。

詳細設定を確認するには、show detail command コマンドを入力します：

```
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 #
```

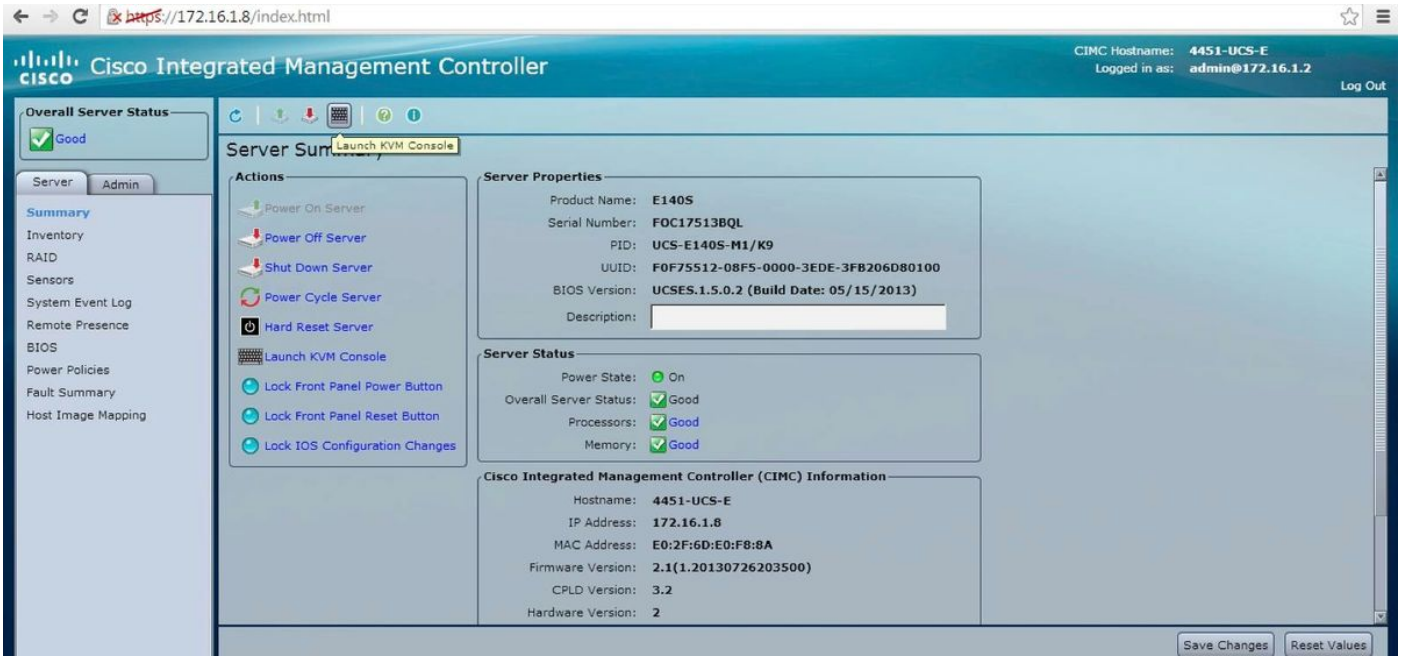
デフォルトのユーザ名とパスワードを使用して、ブラウザから CIMC の Web インターフェイスを起動します。 デフォルトのユーザ名およびパスワードは次のとおりです。

- ユーザ名： **admin**
- パスワード： **password**

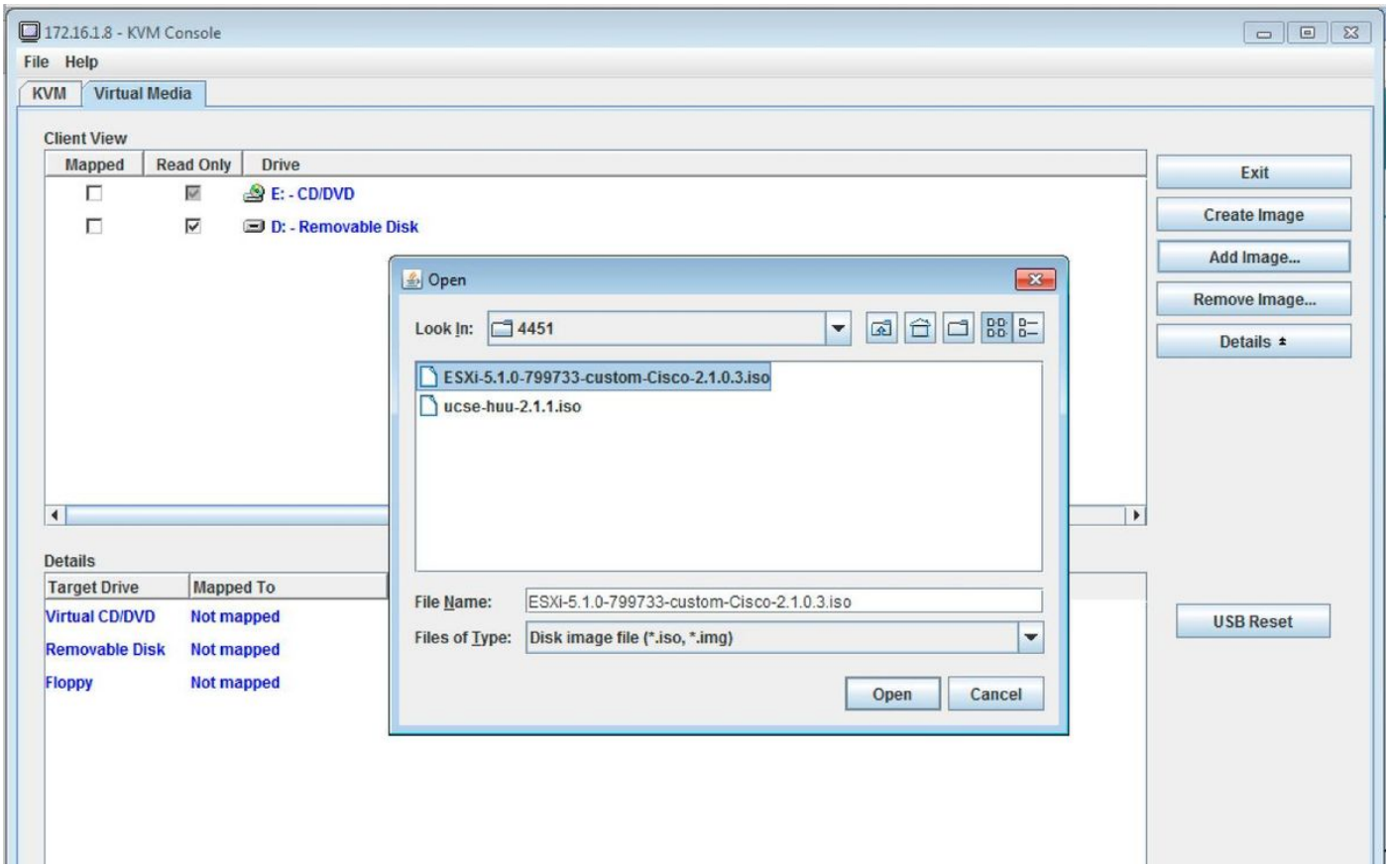



## ESXi のインストール

CIMC のユーザ インターフェイスにログインすると、次の図のようなページが表示されます。 [Launch KVM Console] アイコンをクリックし、[add image] をクリックし、仮想メディアとして ESXi ISO をマッピングします。




[Virtual Media] タブをクリックし、次に [Add Image] をクリックして仮想メディアをマッピングします。




仮想メディアがマッピングされた後、CIMC ホームページから [Power Cycle Server] をクリックし、UCS-E の電源を再投入します。 仮想メディアから ESXi セットアップが起動されます。 ESXi のインストールが完了します。

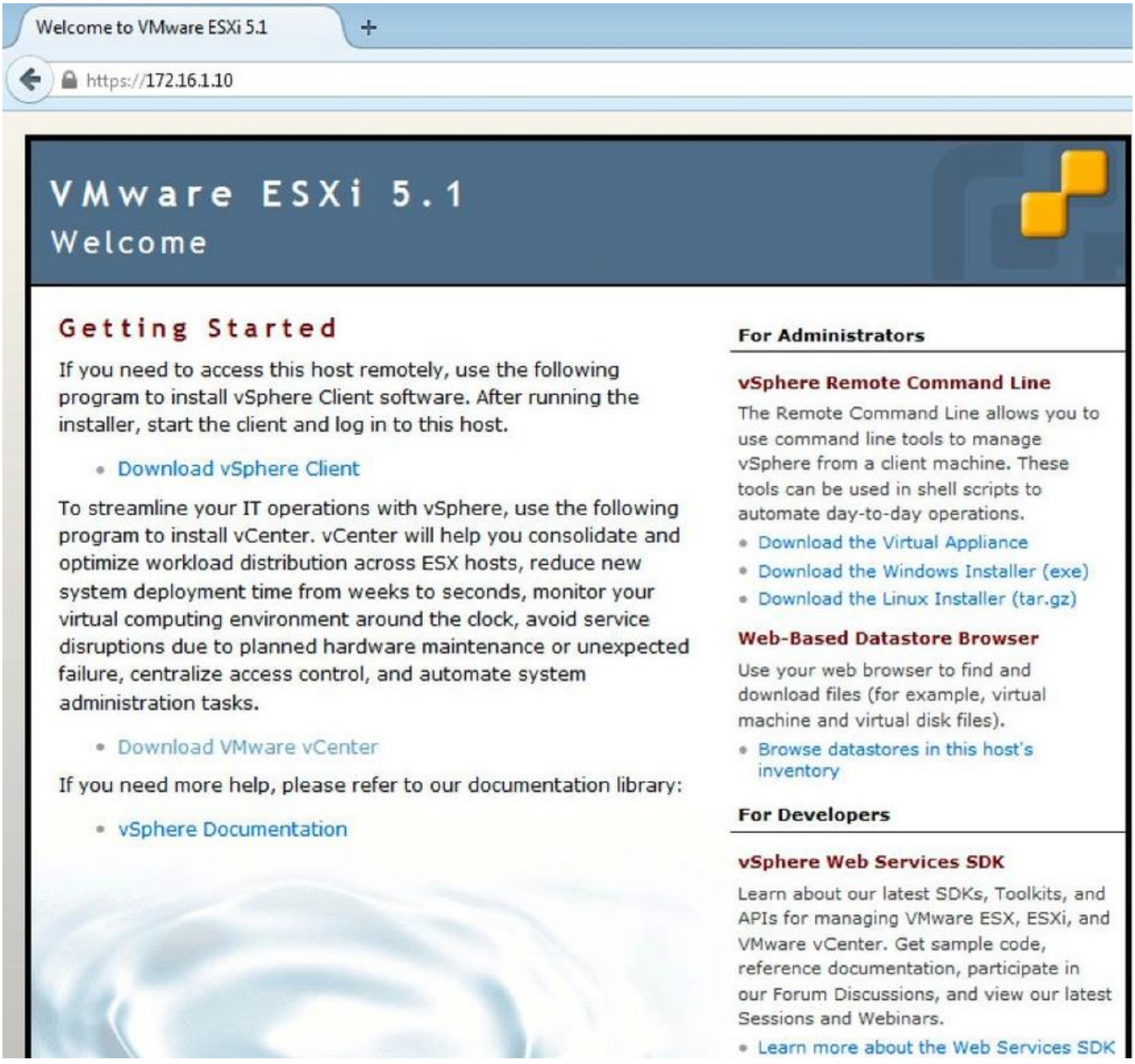
> **注:** 今後の参照用として、*ESXi IP アドレス*、*ユーザ名*、および*パスワード*を記録しておきます。

# vSphere Client のインストール

ここでは、vSphere Client のインストール方法について説明します。

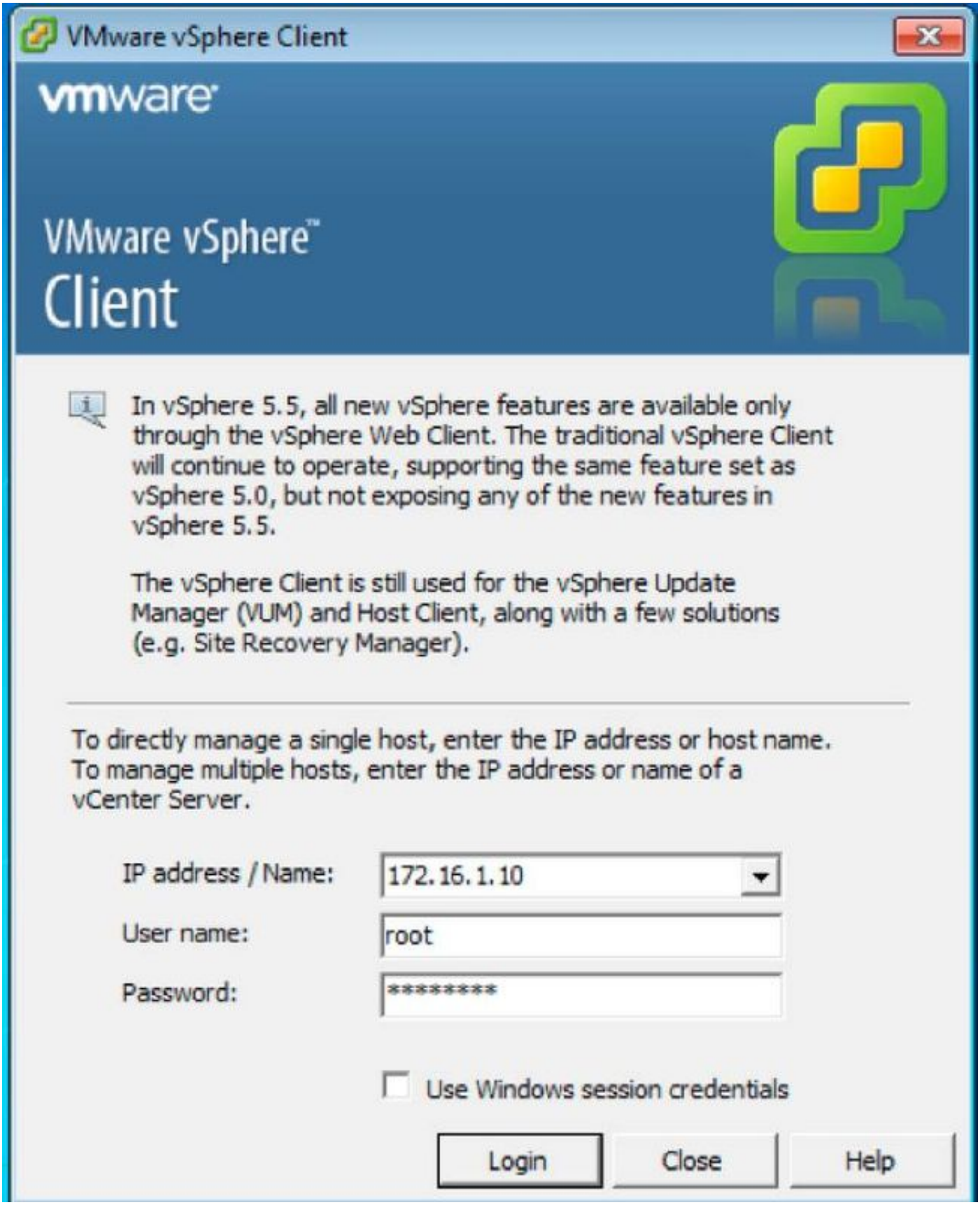
## vSphere Client のダウンロード

ESXi を起動し、[Download VSphere Client] リンクを使用して vSphere Client をダウンロードします。 これをコンピュータにインストールします。




## vSphere Client の起動

コンピュータから vSphere Client を実行します。 インストール中に作成したユーザ名とパスワードでログインします：




### FireSIGHT Management Center および FirePOWER デバイスの展開

ESXi に FireSIGHT Management Center を展開するには、Cisco ドキュメント『VMware ESXi での FireSIGHT Management Center の展開』のにある手順を実行します。

**注:** FirePOWER NGIPSv デバイスを展開するためのプロセスは、Management Center の展

開プロセスと類似しています。

## インターフェイスの設定

デュアル幅 UCS-E には 4 つのインターフェイスがあります：

- 最も高い MAC アドレス インターフェイスは前面パネルにある Gi3 です。
- 2 番目に高い MAC アドレス インターフェイスは前面パネルにある Gi2 です。
- 最後の 2 つのインターフェイスは、内部インターフェイスです。

シングル幅 UCS-E には、3 つのインターフェイスがあります：

- 最も高い MAC アドレス インターフェイスは前面パネルにある Gi2 です。
- 最後の 2 つのインターフェイスは、内部インターフェイスです。

ISR4K にある UCS-E インターフェイスはどちらもトランク ポートです。

UCS-E 120S および 140S には 3 つのネットワーク アダプタと管理ポートがあります：

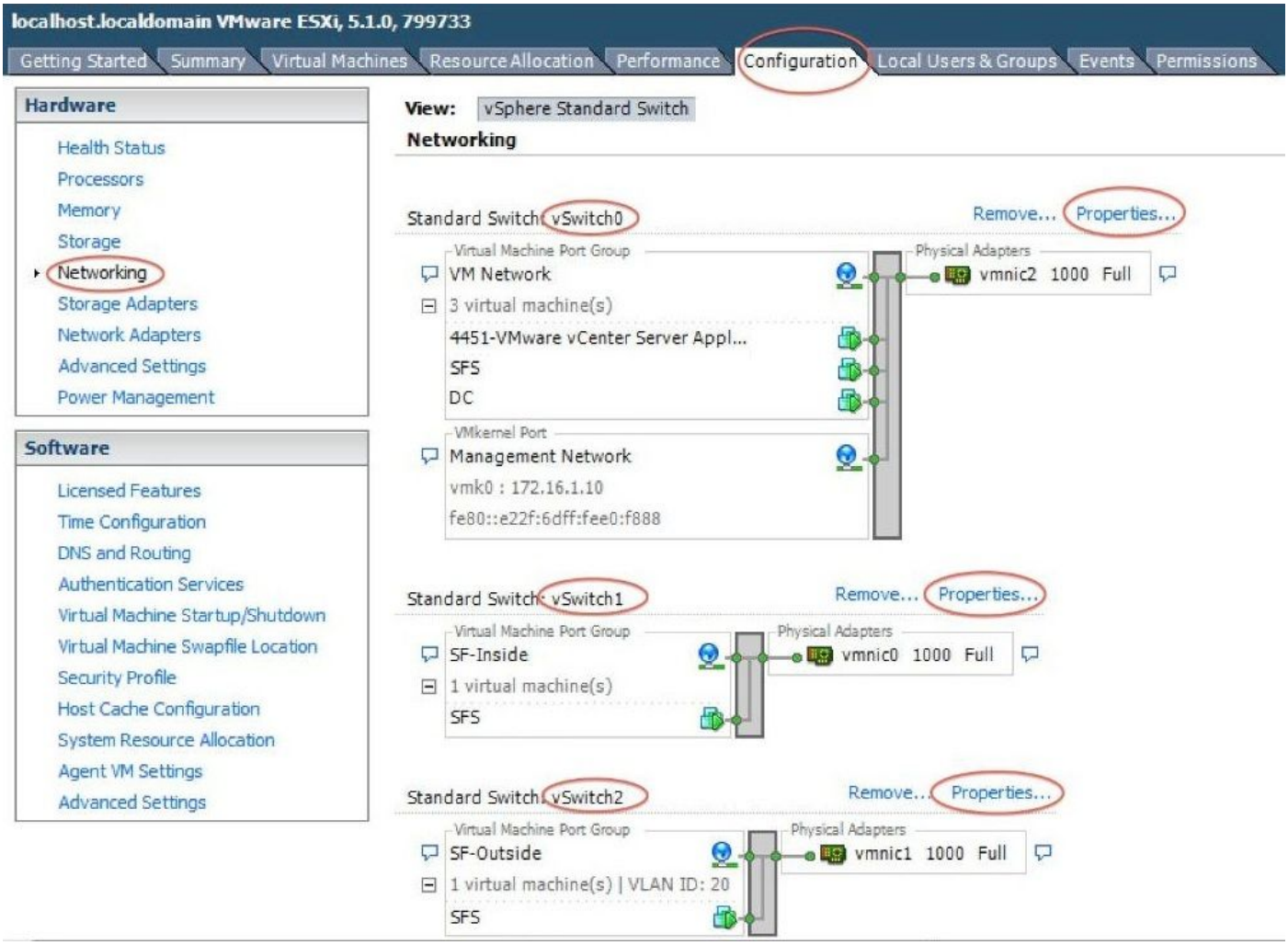
- *vmnic0* はルータ バックプレーンの *UCSEx/0/0* にマッピングされます。
- *vmnic1* はルータ バックプレーンの *UCSEx/0/1* にマッピングされます。
- *vmnic2* は UCS-E フロント プレーン GE2 インターフェイスにマッピングされます。
- 前面パネル管理（M）ポートは、CIMC のみに使用できます。

UCS-E 140D、160D および 180D には 4 つのネットワーク アダプタがあります：

- *vmnic0* はルータ バックプレーンの *UCSEx/0/0* にマッピングされます。
- *vmnic1* はルータ バックプレーンの *UCSEx/0/1* にマッピングされます。
- *vmnic2* は UCS-E フロント プレーン GE2 インターフェイスにマッピングされます。
- *vminc3* は UCS-E のフロント プレーン GE3 インターフェイスにマッピングされます。
- 前面パネル管理（M）ポートは、CIMC のみに使用できます。

### ESXi での vSwitch インターフェイスの設定

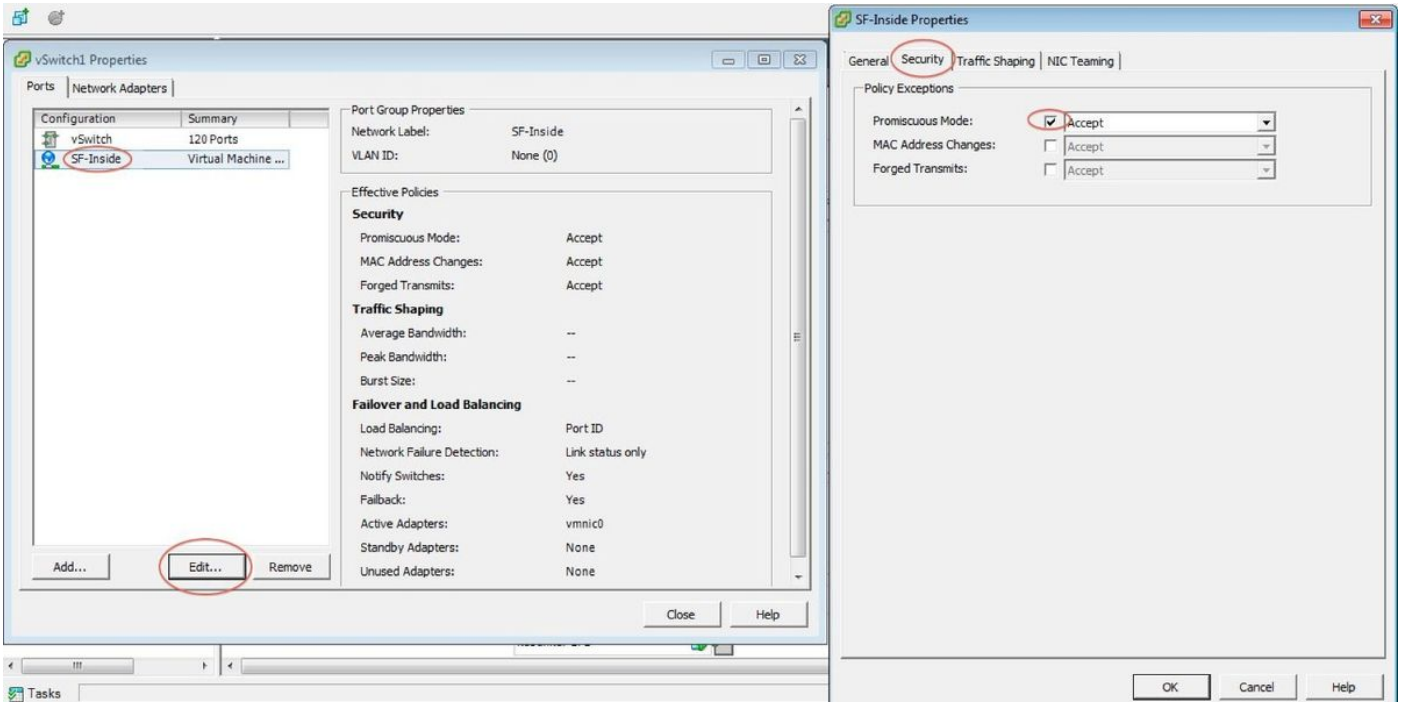
ESXi 上の vSwitch0 は、ESXi、FireSIGHT Management Center、および FirePOWER NGIPSv デバイスがネットワークと通信するために使われる管理インターフェイスです。 vSwitch1（SF-Inside）と vSwitch2（SF-Outside）の [Properties] をクリックして、変更を加えます。




次の図に、vSwitch1 のプロパティを示します（vSwitch2 についても同じ手順を行う必要があります）。

**注: VLAN ID を設定されます NGIPSv のための 4095 に、これ必要とされます NGIPSv 資料に従って確認して下さい:**

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



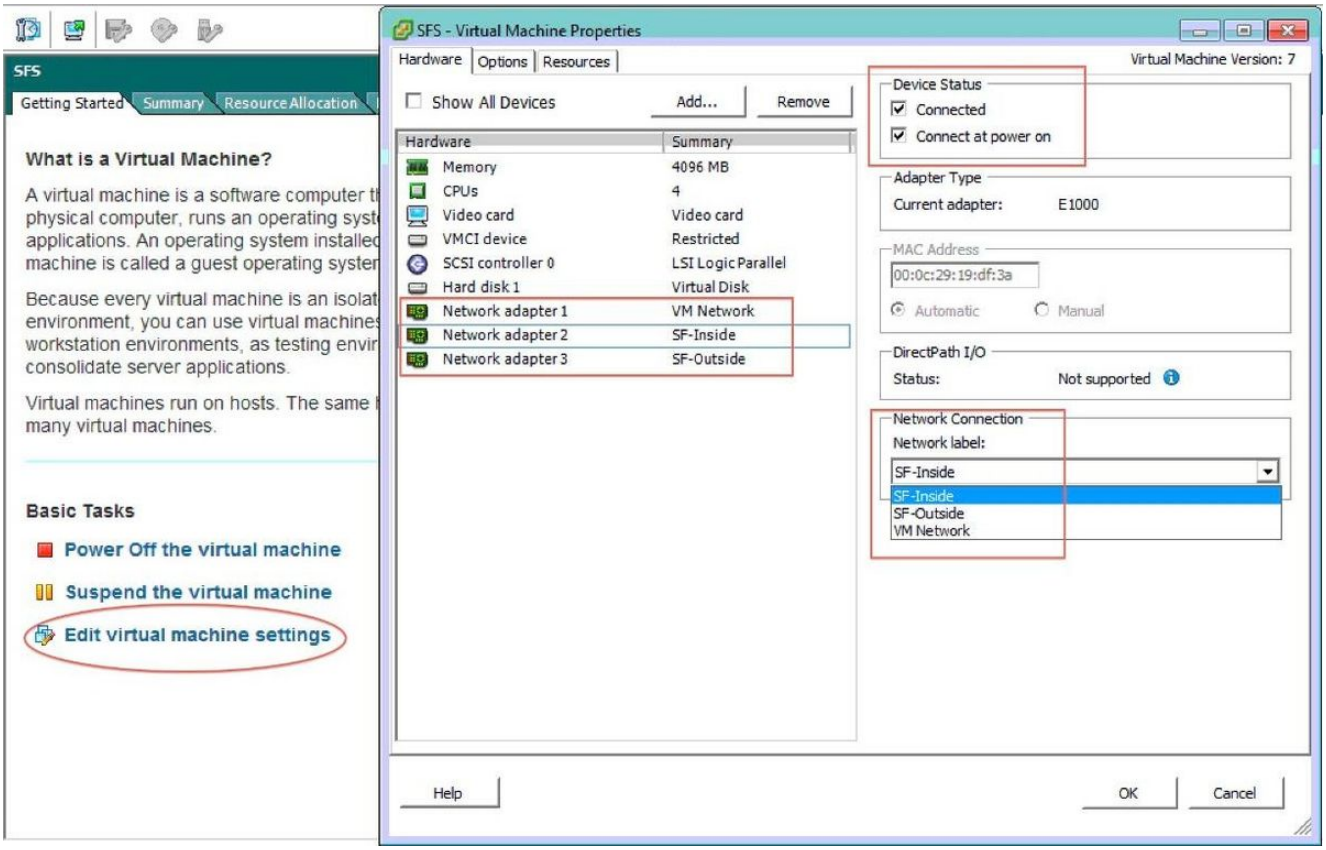

ESXi 上の vSwtich 設定が完了しました。 次に、インターフェイスの設定を確認する必要があります：

1. FirePOWER デバイスの仮想マシンに移動します。

2. [Edit virtual machine settings] をクリックします。

3. 3 つのネットワーク アダプタをすべて確認します。

4. 次のように正しく選択されていることを確認してください。




### FireSIGHT Management Center への FirePOWER デバイスの登録

Cisco ドキュメントに記載されている手順を完了し、FirePOWER デバイスを FireSIGHT Management Center に登録します。

## トラフィックのリダイレクトと確認

このセクションでは、トラフィックをリダイレクトする方法とパケットを確認する方法について説明します。

### ISR から UCS-E 上のセンサーへのトラフィックのリダイレクト

トラフィックのリダイレクトには次の情報を使用します。

```
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
```

> **注:** バージョン 3.16.1 以降を現在実行している場合は、utd コマンドではなく utd engine advanced コマンドを使用してください。

### パケット リダイレクションの確認

パケット カウンタが増加しているかどうか確認するには、ISR コンソールから次のコマンドを入力します。

```
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
```

## 確認

次の show コマンドを使用して、設定が正しく機能するかどうかを確認できます。

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

## トラブルシューティング

次の debug コマンドを使用して、設定のトラブルシューティングを行うことができます。

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

# 関連情報

- Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジン スタートアップ ガイド リリース 2.x
- Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジンのトラブルシューティング ガイド
- Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジン スタートアップ ガイド リリース 2.x – ファームウェアのアップブレード
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ ソフトウェア コンフィギュレーション ガイド – ブリッジ ドメイン インターフェイスの設定
- Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジンのホスト アップグレード ユーティリティ ガイド – Cisco UCS E シリーズ サーバでのファームウェアのアップグレード
- テクニカル サポートとドキュメント – Cisco Systems