UCS-E ブレードが付いている ISR デバイスの設定 FirePOWER サービス

目次

概要

この資料に Intrusion detection system （ IDS ） モードで Cisco Unified Computing System E シリーズ (UCS-E) ブレード プラットフォームで Cisco FirePOWER ソフトウェアをインストールし展開する方法を記述されています。 この資料に説明がある設定例は公式 ユーザガイドへ補足です。

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 統合サービス ルータ（ISR）XE イメージ 3.14 か以降
- Cisco Integrated Management Controller （CIMC）バージョン 2.3 または それ 以降
- Cisco FireSIGHT Management Center （FMC）バージョン 5.2 または それ 以降
- Cisco FirePOWER 仮想デバイス（NGIPSv）バージョン 5.2 または それ 以降
- VMware ESXi バージョン 5.0 または それ 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

> **注:** バージョン 3.14 または それ 以降にコードをアップグレードする前に、システムにアップグレードのための十分なメモリ、ディスク空間およびライセンスがあることを確認して下さい。 Example 1:参照して下さい: TFTP サーバから flash: へイメージを アクセスルータ ソフトウェアアップグレード手順 Ciscoドキュメントの TFTPサーバ セクションから詳細をコードアップグレードについて学ぶため。

> **注:** CIMC を、BIOS アップグレードするためにおよび他のファームウェア コンポーネント、Cisco ホスト アップグレード ユーティリティ（HUU）を使用できますまたはファームウェア コンポーネントを手動でアップグレードできます。 詳細をファームウェア アップグレードについて学ぶために、on Cisco Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク計算エンジンのためのホスト アップグレード ユーティリティ ユーザガイドのファームウェア UCS E シリーズ サーバ セクションをアップグレードすることを参照して下さい。

背景説明

このセクション サポートされたハードウェアプラットフォームについての情報を、ライセンスおよび制限はこの資料に説明がある手順およびコンポーネントに関して提供します。

サポートされたハードウェアプラットフォーム

このセクションは G2 および 4000 シリーズ デバイスのためのサポートされたハードウェアプラットフォームをリストします。

UCS-E ブレードが付いている ISR G2 デバイス

UCS-E シリーズ ブレードが付いているこれらの ISR G2 シリーズ デバイスはサポートされます:

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 単一広いオプション
	2921	UCS-E 120/140/160/180 シングルまたはダブル広いオプショ
	2951	UCS-E 120/140/160 シングルまたはダブル広いオプション
Cisco 3900 シリーズ ISR	3925	UCS-E 120/140/160 単一および二重広いオプションか 180 番重広い
	3925E	UCS-E 120/140/160 単一および二重広いオプションか 180 番重広い
	3945	UCS-E 120/140/160 単一および二重広いオプションか 180 番重広い
	3945E	UCS-E 120/140/160 単一および二重広いオプションか 180 番重広い

UCS-E ブレードが付いている ISR 4000 デバイス

UCS-E シリーズ ブレードが付いているこれらの ISR 4000 シリーズ デバイスはサポートされます:

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 単一および二重広いオプションか 180 番重広い
	4431	UCS-E ネットワーク インターフェース インタフェース・モジル
Cisco 4300 シリーズ ISR	4351	UCS-E 120/140/160/180 単一および二重広いオプションか 180二重広い
	4331	UCS-E 120/140 単一広いオプション
	4321	UCS-E ネットワーク インターフェース インタフェース・モジル

ライセンス

ISR はセキュリティ K9 ライセンス、またサービスを有効に するために appx ライセンスがなければなりません。

制限事項

2 つの制限は情報に関してここにありますこの資料に説明がある:

- マルチキャストはサポートされません
- 4,096 のブリッジドメイン インターフェイスだけ（BDI）各システムのためにサポートされます

BDIs はこれらの機能をサポートしません:

- 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）か高度ビデオ符号化（AVC）
- ゾーンは基づかせていましたファイアウォール（ZBF）を
- 暗号 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 ）

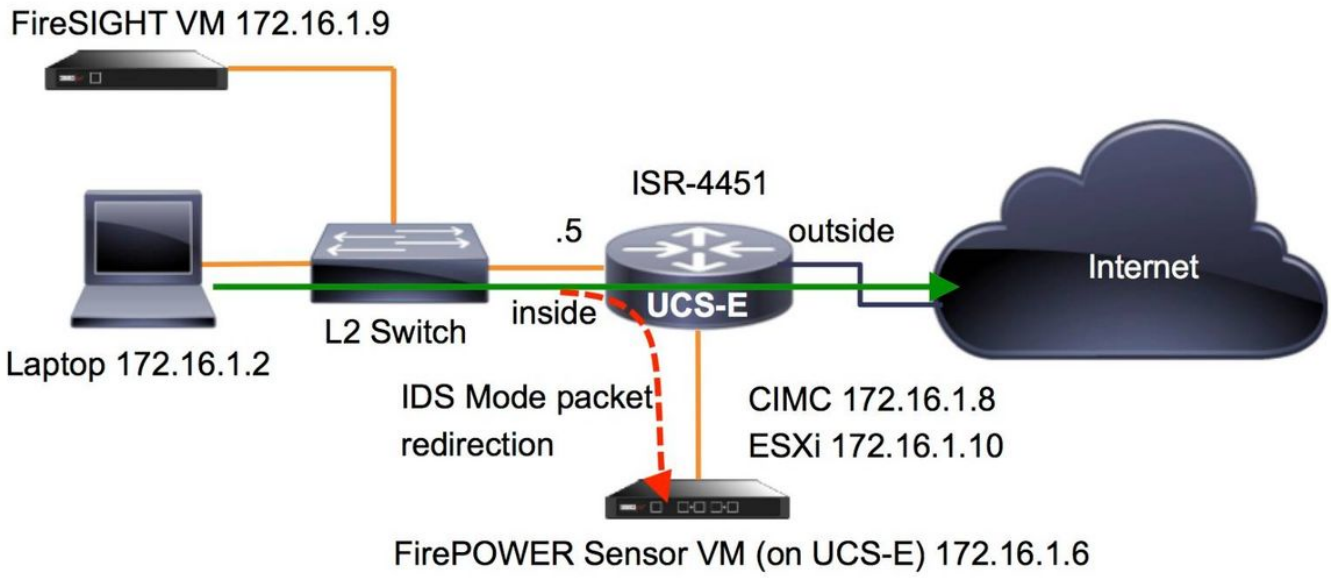
  注: BDI の場合、最大伝送ユニット （ MTU ）サイズは 1,500 のおよび 9,216 バイト間のあらゆる値で設定することができます。

設定

このセクションはこの配備に関連するコンポーネントを設定する方法を記述します。

ネットワーク図

設定はこの資料に説明があるこのネットワーク・トポロジを使用します:



UCS-E の FirePOWER サービスのための作業の流れ

UCS-E で動作する FirePOWER サービスのための作業の流れはここにあります:

1. データプレーンは BDI/UCS-E インターフェイスからのインスペクション用のトラフィックを押します (G2 および G3 シリーズ デバイスのためにはたらきます) 。
2. Cisco IOS®-XE CLI は分析 (すべてのインターフェイスのためのオプションかインターフェースごと) のためのパケット リダイレクションをアクティブにします。
3. センサー CLI **設定**スタートアップスクリプトは設定を簡約化します。

設定 CIMC

このセクションは CIMC を設定する方法を記述します。

CIMC への接続応答

CIMC に接続する複数の方法があります。 この例では、CIMC への接続は専用管理ポートによって完了します。 イーサネット ケーブルの使用とネットワークに M ポートを (専用されている

) 接続するようにして下さい。 接続される、ルータプロンプトから **hw-module サブスロット** コマンドを実行して下さい:

```
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
```

助言 1: 終了するために、**^a^q.を**実行して下さい。

助言 2: デフォルトのユーザ名は **admin** およびパスワード <password> です。 パスワードリセットプロセスはここに説明されます : 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

設定 CIMC

CIMC の設定を完了するためにこの情報を使用して下さい:

```
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： 変更を保存するために **commit コマンドを**実行すること Enure。

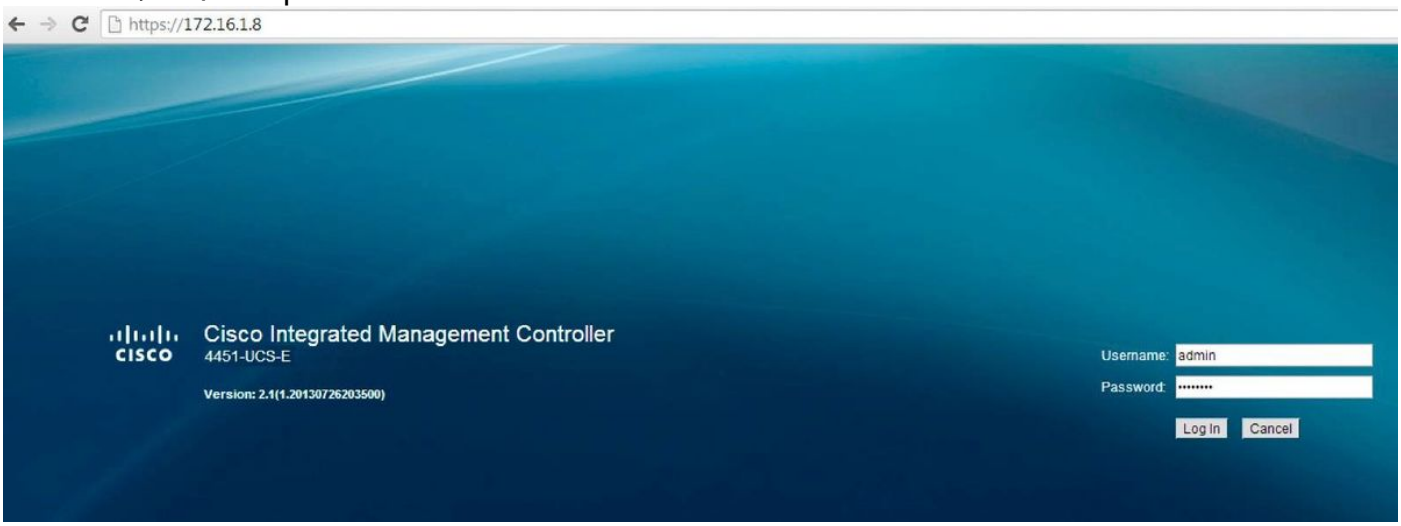
注: モードは管理ポートが使用されるとき**専用**設定 されます。

詳細設定を確認するために**提示 detail コマンドを**実行して下さい:

```
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 #
```

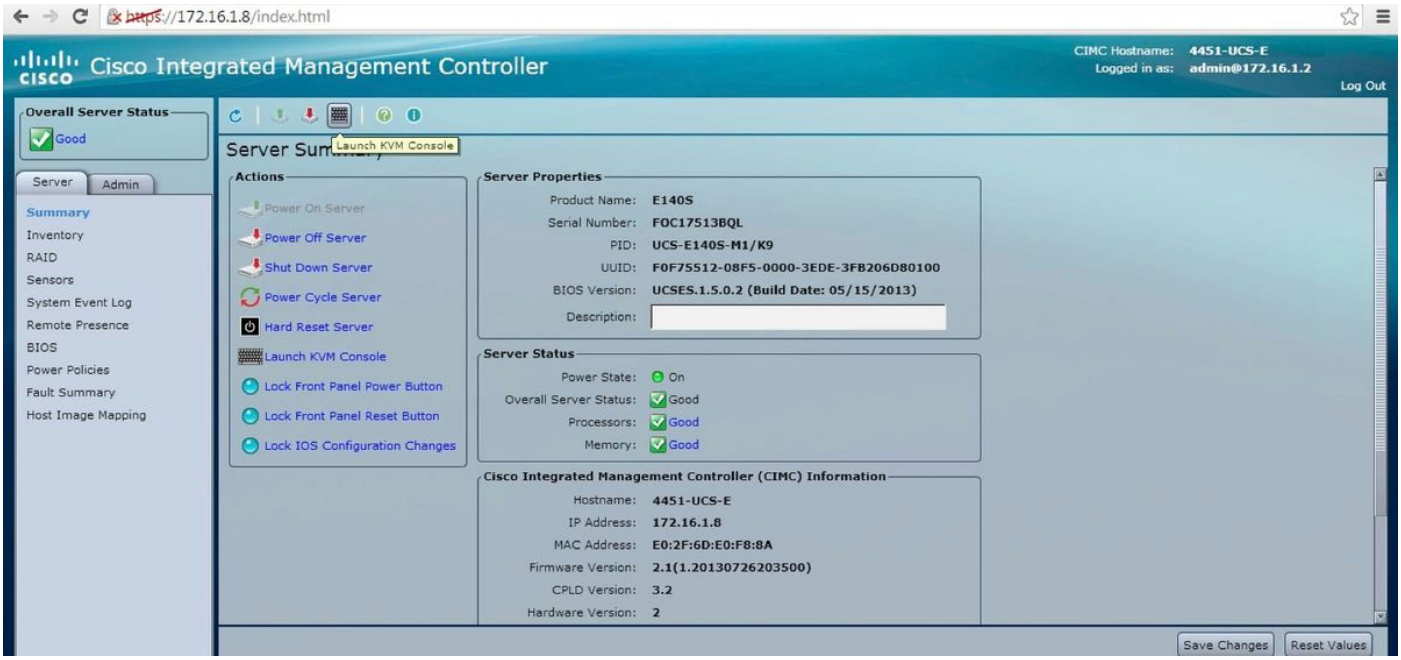
イメージに示すようにデフォルトのユーザ名とブラウザおよびパスワードからの CIMC の Webインターフェイスを起動させて下さい。 デフォルトのユーザ名およびパスワードは次のとおりです:

- ユーザ名： admin
- パスワード： <password>

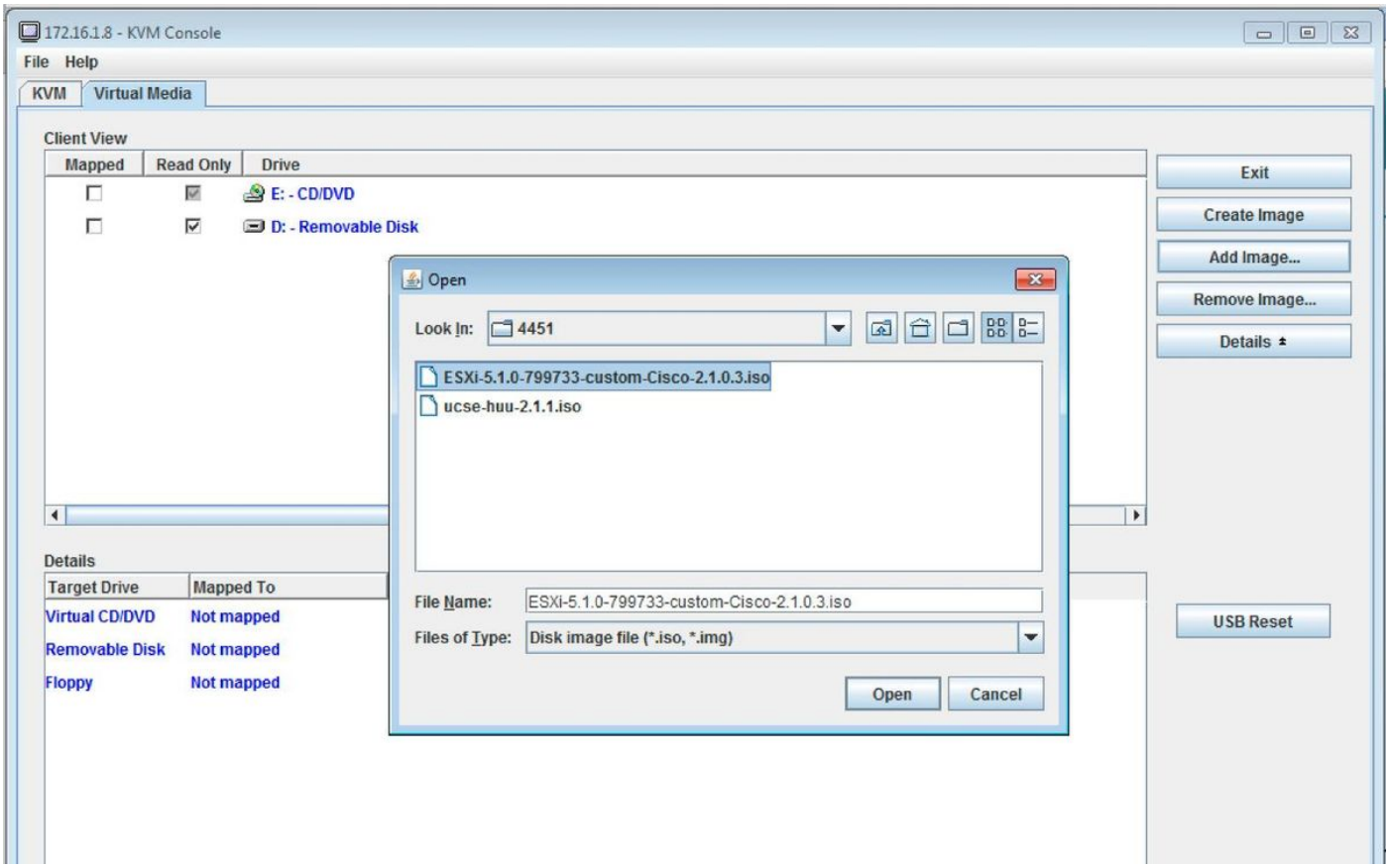


ESXi をインストールして下さい

CIMC のユーザインターフェイスに記録 した後、このイメージで示されているそれと同じようなページを表示できます。 **起動 KVM Console アイコンを**クリックし、**イメージを**『Add』 をクリック し、次にバーチャル メディアとして ESXi ISO をマップして下さい:



バーチャル Media タブをクリックし、次にイメージに示すようにバーチャル メディアをマップするために**イメージを**『Add』 をクリック して下さい。



バーチャル メディアがマップされた後、UCS-E のパワーサイクルを行うために CIMC ホームページからの**電源の再投入 サーバを**クリックして下さい。 ESXi 設定はバーチャル メディアから起動します。 ESXi インストールを完了して下さい。

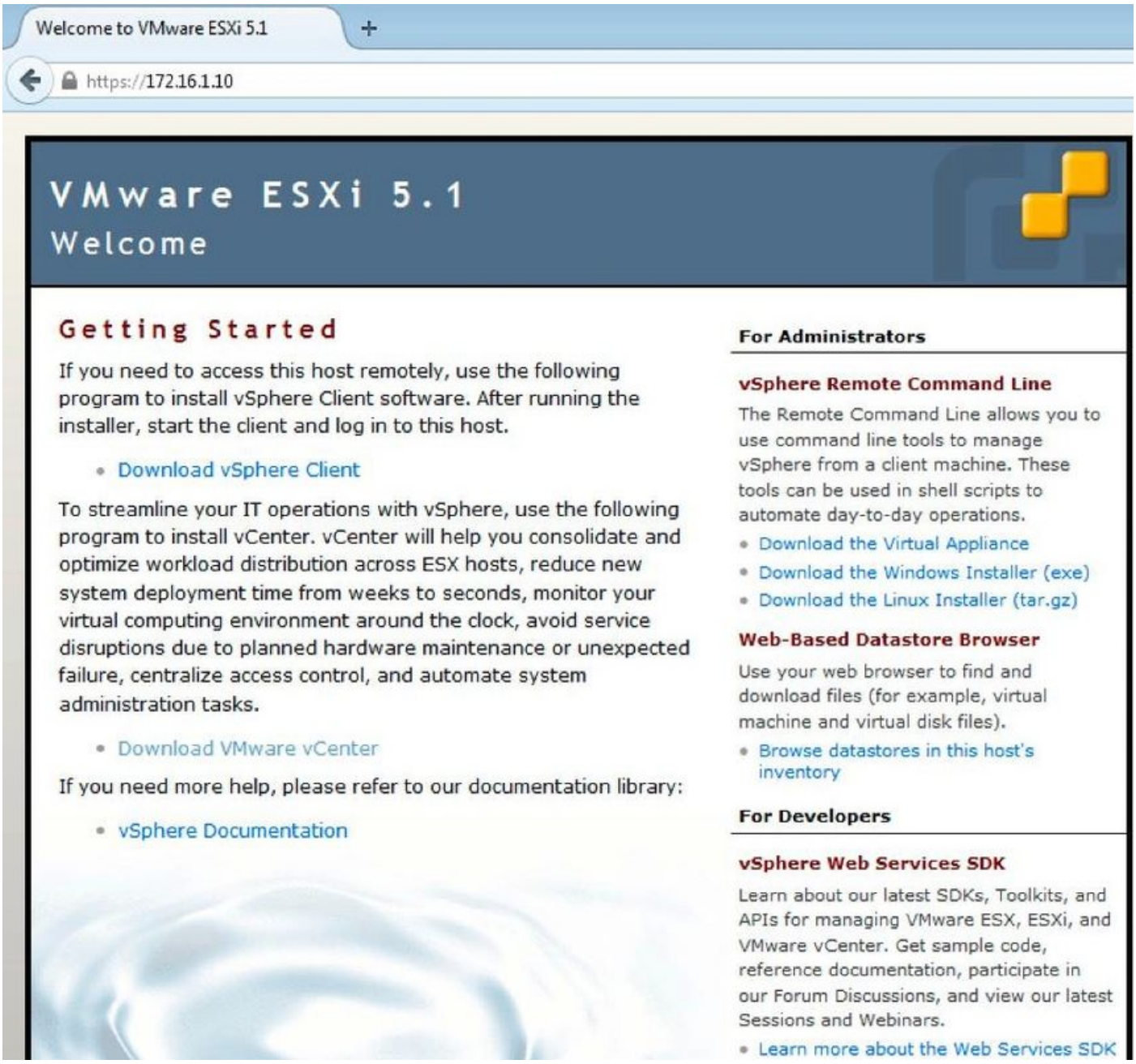
注: 未来の参照用の ESXi IP アドレス、ユーザー名およびパスワードを書き留めて下さい。

vSphere クライアントをインストールして下さい

このセクションは vSphere クライアントをインストールする方法を記述します。

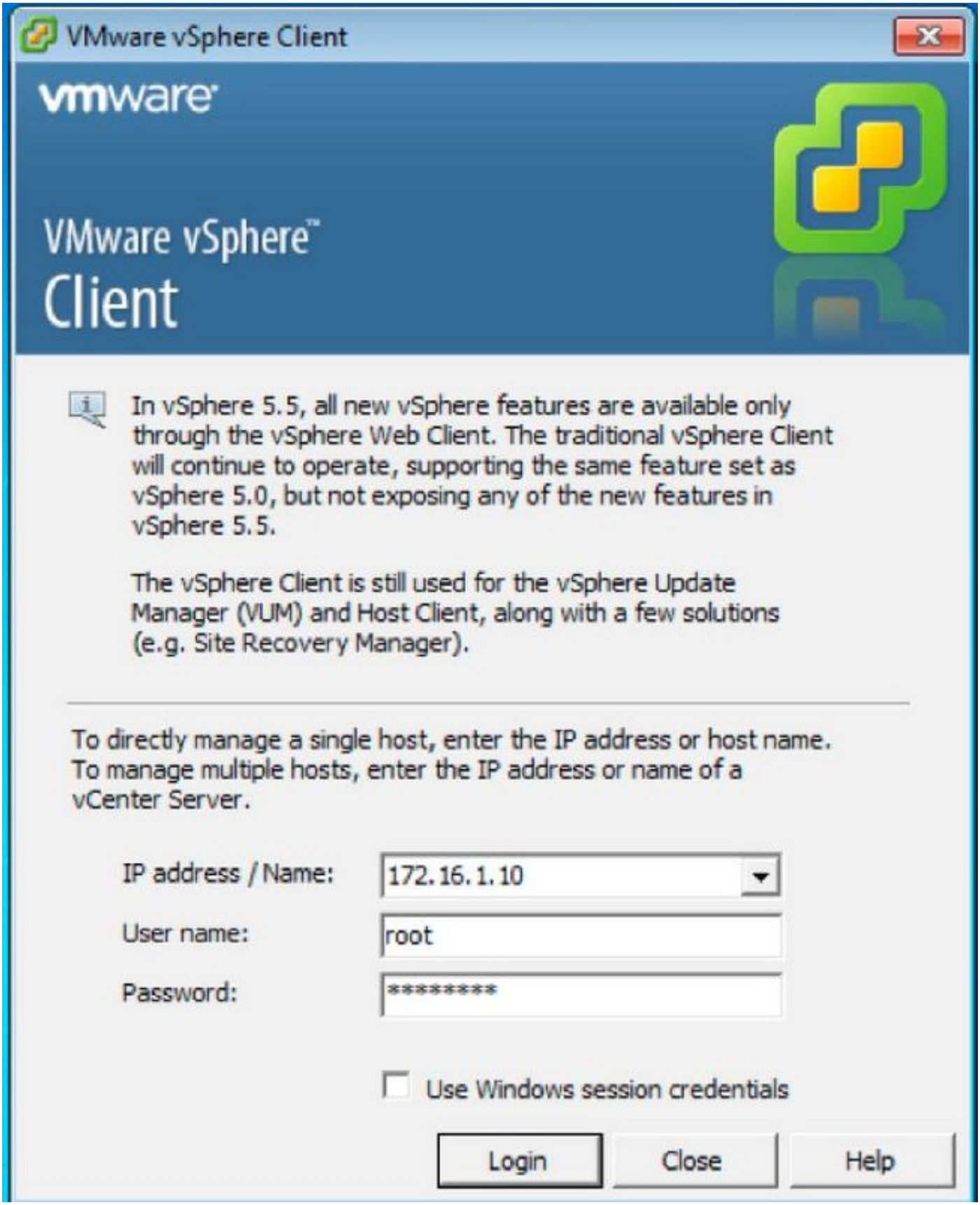
ダウンロード vSphere クライアント

ESXi を起動させ、vSphere クライアントをダウンロードするために**ダウンロード VSphere クライアント** リンクを使用して下さい。 コンピュータでそれをインストールして下さい。



vSphere クライアントを起動させて下さい

コンピュータから vSphere クライアントを起動させて下さい。 インストールの間におよびイメージに示すように作成したユーザ名 および パスワードのログイン:



導入 FireSIGHT Management Center および FirePOWER デバイス

ESXi の FireSIGHT Management Center を展開するために VMware ESXi Ciscoドキュメントの FireSIGHT Management Center の配備に説明がある手順を完了して下さい。

注: プロセスは FirePOWER NGIPSv デバイスを配置するために使用するプロセスに類似し

たです管理 センターを配置するために使用される。

インターフェイス

デュアル ワイド UCS-E で、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の Gi3 です
- 第 2 最も高い MAC アドレス インターフェイスは前面パネルの Gi2 です
- 現われる最後の 2 つは内部インターフェースです

シングル ワイド UCS-E で、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の Gi2 です
- 現われる最後の 2 つは内部インターフェースです

ISR4K の UCS-E インターフェイスの両方はトランク ポートです。

UCS-E 120S および 140S に管理ポートと 3 ネットワーク アダプタがあります:

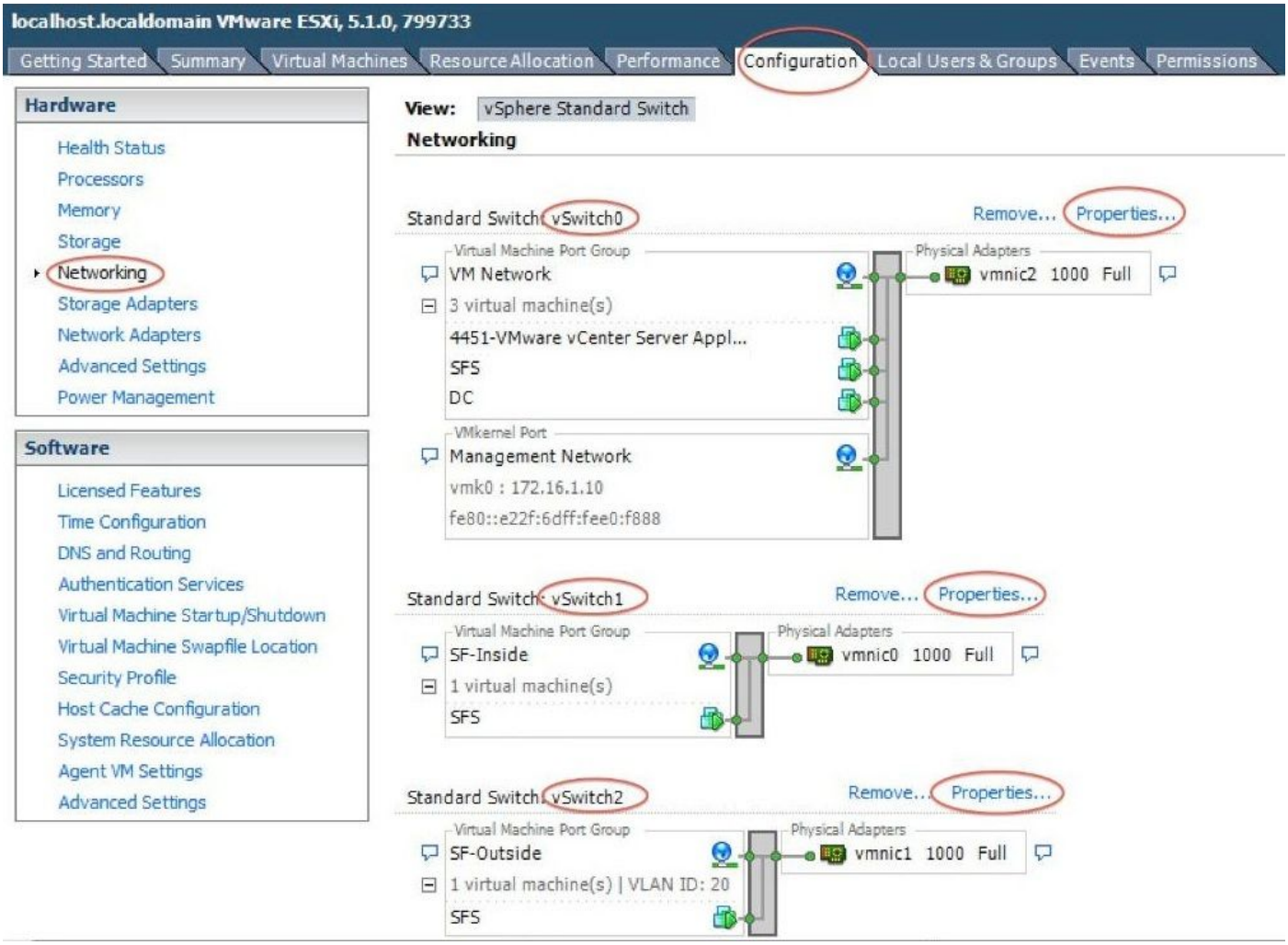
- *vmnic0 は*ルータ バックプレーンの *UCSEx/0/0* にマップされます
- *vmnic1 は*ルータ バックプレーンの *UCSEx/0/1* にマップされます
- *vmnic2 は* UCS-E 先頭平面 GE2 インターフェイスにマップされます
- 前面パネル管理（m）ポートは CIMC のためにしか使用することができません。

UCS-E 140D、160D および 180D に 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* にマップされます。
- *vmnic1 は*ルータ バックプレーンの *UCSEx/0/1* にマップされます。
- *vmnic2 は* UCS-E 先頭平面 GE2 インターフェイスにマップされます。
- *vminc3 は* UCS-E 先頭平面 GE3 インターフェイスにマップされます。
- 前面パネル管理（m）ポートは CIMC のためにしか使用することができません。

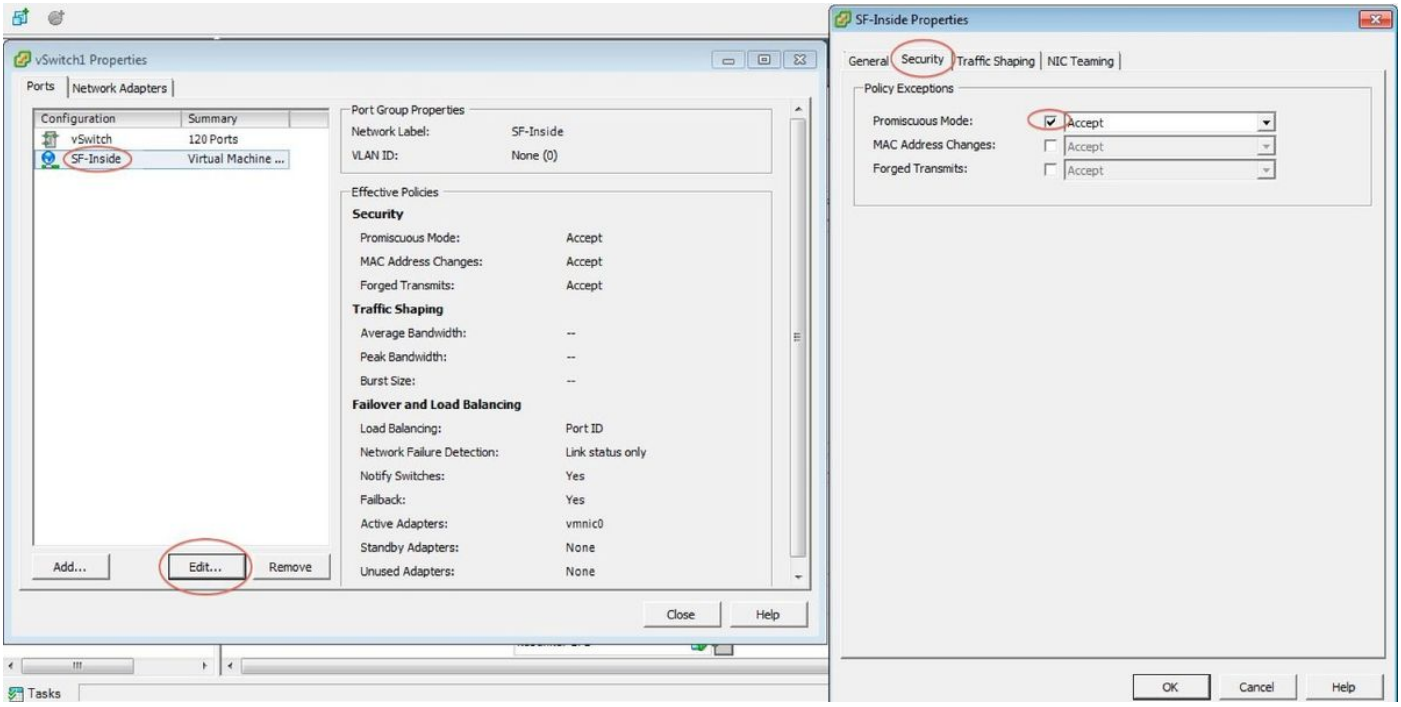
ESXi の vSwitch インターフェイス

ESXi 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管理インターフェイスです。 変更を行なうために vSwitch1（SF の中で）および vSwitch2（SF 外部）のために『Properties』 をクリック して下さい。



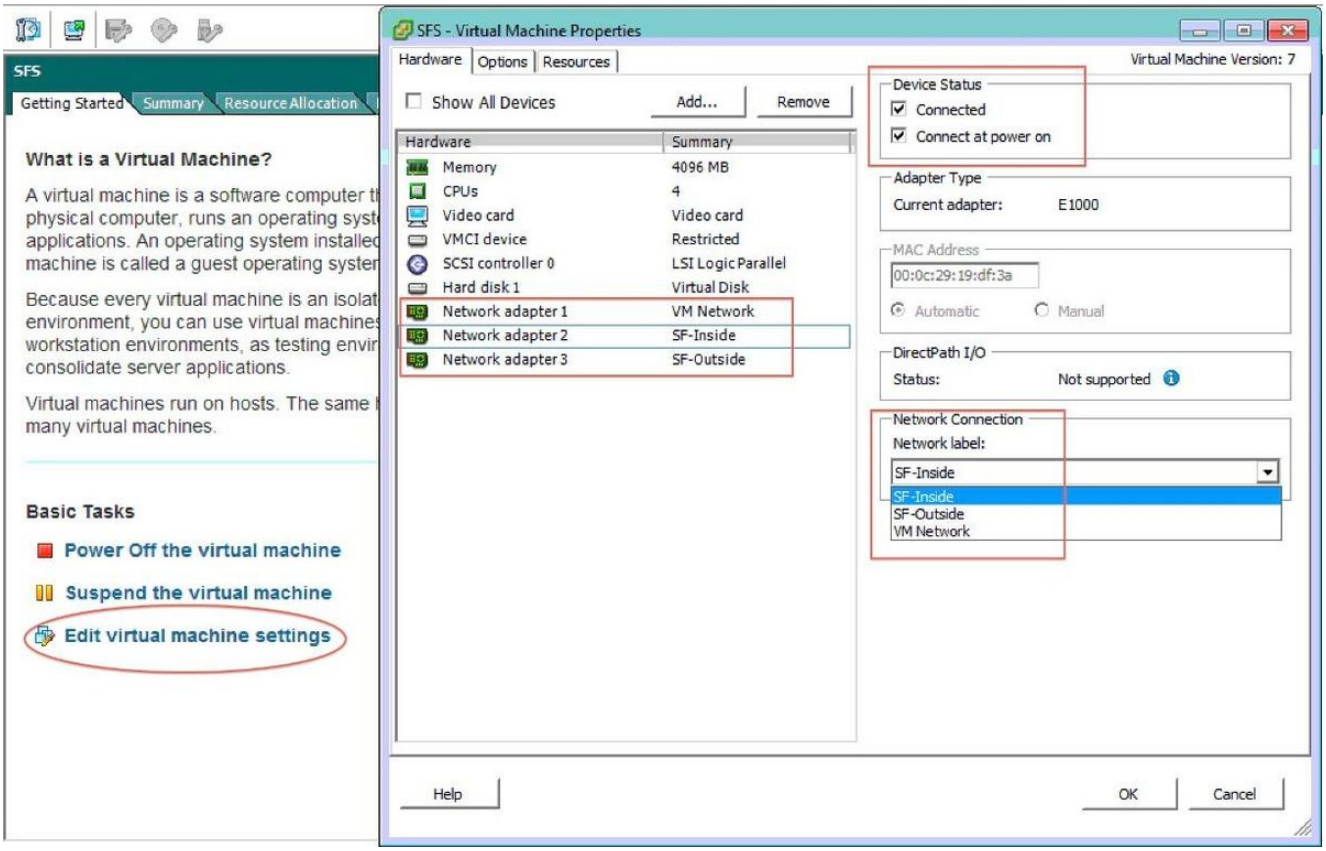
このイメージは vSwitch1 （vSwitch2 のための同じステップを完了して下さい）のプロパティを示します:

> **注:** これが NGIPSv 資料に従って必要となることをように VLAN ID 設定される NGIPSv のための 4095 にして下さい: http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



ESXi の vSwtich 設定は完了しました。 この場合インターフェイス設定を確認して下さい:

1. FirePOWER デバイスのための仮想マシンにナビゲートして下さい。
2. **仮想マシン設定を**『Edit』 をクリック して下さい。
3. 3 つのネットワーク アダプタすべてを確認して下さい。
4. それらがきちんと選択されるここのイメージに示すようにように、して下さい:



FireSIGHT Management Center の FirePOWER デバイスを登録して下さい

FireSIGHT Management Center の FirePOWER デバイスを登録するために Ciscoドキュメントに

説明がある手順を完了して下さい。

トラフィックをリダイレクトし、確認して下さい

このセクションでは、設定が正常に機能していることを確認します。

このセクションはトラフィックをリダイレクトする方法をおよびパケットを確認する方法を記述します。

ISR からの UCS-E のセンサーへのリダイレクト トラフィック

トラフィックをリダイレクトするためにこの情報を使用して下さい:

```
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:** 現在 バージョン 3.16.1 または それ 以降を実行する場合、**UTD** コマンドの代りに **UTD エンジンによって進められる**コマンドを実行して下さい。

パケット リダイレクションを確認して下さい

ISR コンソールから、パケット カウンターが増分するかどうか確かめるためにこのコマンドを実行して下さい:

```
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

設定がきちんと機能することを確認するためにこれらの **show コマンドを**実行できます:

- **地図をつくりますグローバル な ソフトウェア UTD の示して下さい**
- **地図をつくりますソフトウェア UTD インターフェイスの示して下さい**
- **地図をつくりますグローバル な ソフトウェア UTD RP アクティブの示して下さい**
- **地図をつくりますグローバル な ソフトウェア UTD fp アクティブの示して下さい**
- **地図をつくりますハードウェア qfp のアクティブな機能 UTD 統計示して下さい**
- **プラットフォーム ハードウェア qfp にアクティブな機能 UTD を示して下さい**

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

設定をトラブルシューティングするためにこれらの **debug コマンドを**実行できます:

- **デバッグ プラットフォーム状態機能 UTD controlplane**
- **デバッグ プラットフォーム状態機能 UTD dataplane サブモード**

関連情報

- Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク計算エンジンのためのガイドの開始、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 ネットワーク計算エンジンのため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 ネットワーク計算エンジンのためのガイドを開始します、リリース 2.x –ファームウェアをアップグレードすること
- 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 ネットワーク計算エンジンのためのホスト アップグレード ユーティリティ ユーザガイド–ファームウェア UCS E シリーズ サーバを on Cisco アップグレードすること
- テクニカル サポートとドキュメント – Cisco Systems