

# 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

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[サポートされたハードウェアプラットフォーム](#)

[UCS-E ブレードが付いている ISR G2 デバイス](#)

[UCS-E ブレードが付いている ISR 4000 デバイス](#)

[ライセンス](#)

[制限事項](#)

[設定](#)

[ネットワーク図](#)

[UCS-E の FirePOWER サービスのための作業の流れ](#)

[設定 CIMC](#)

[CIMC への接続応答](#)

[設定 CIMC](#)

[ESXi をインストールして下さい](#)

[vSphere クライアントをインストールして下さい](#)

[vSphere クライアントをダウンロードして下さい](#)

[vSphere クライアントを起動させて下さい](#)

[FireSIGHT Management Center および FirePOWER デバイスを配置して下さい](#)

[インターフェイス](#)

[ESXi の vSwitch インターフェイス](#)

[FireSIGHT Management Center のレジスタ FirePOWER デバイス](#)

[トラフィックをリダイレクトし、確認して下さい](#)

[ISR から UCS-E のセンサーにトラフィックをリダイレクトして下さい](#)

[パケットリダイレクションを確認して下さい](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 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され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: ハイイメージを](#) 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ン
	2951	UCS-E 120/140/160 シングルまたはダブル広いオプション
	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
Cisco 3900 シリーズ ISR	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
	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
Cisco 4300 シリーズ ISR	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が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 )

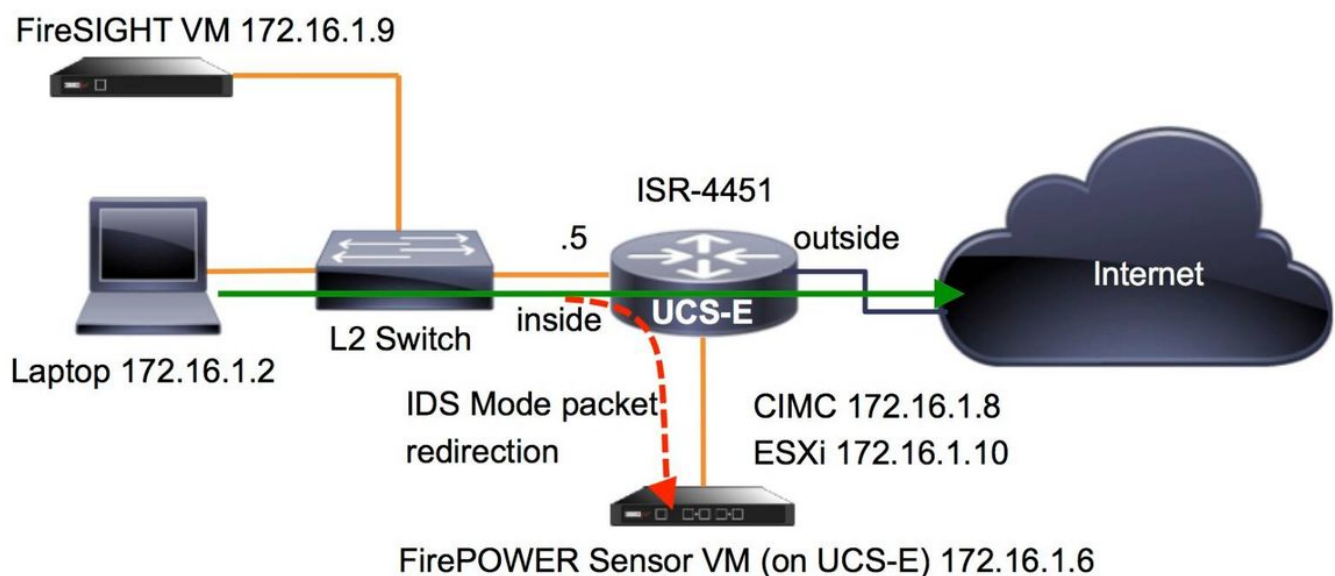
注: BDI の場合、最大伝送ユニット ( MTU ) サイズは 1,500 のおよび 9,216 バイト間のあらゆる値で設定することができます。

## 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 있습니다:

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きません )。
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がインターフェイスごと ) 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/guide/b\\_Getting\\_Started\\_Guide/b\\_3\\_x\\_Getting\\_Started\\_Guide\\_appendix\\_01011.html#GUID-73551F9A-4C79-4692-838A-F99C80E20A28](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/3-1-1/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

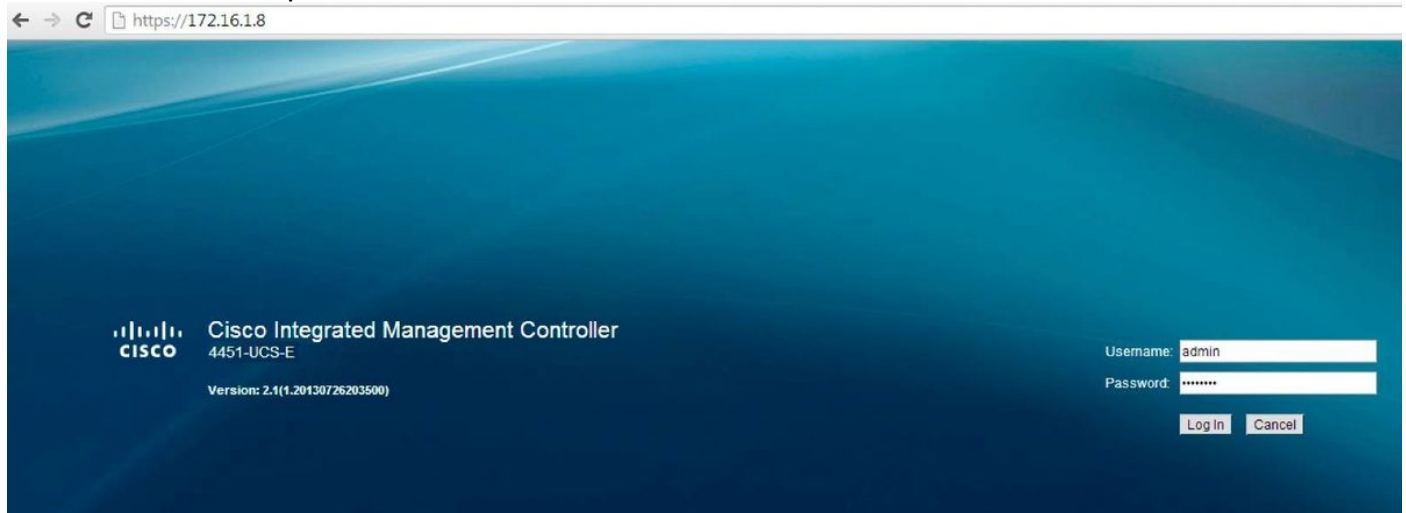
NIC Redundancy: none

NIC Interface: console

```
4451-UCS-E /cimc/network #
```

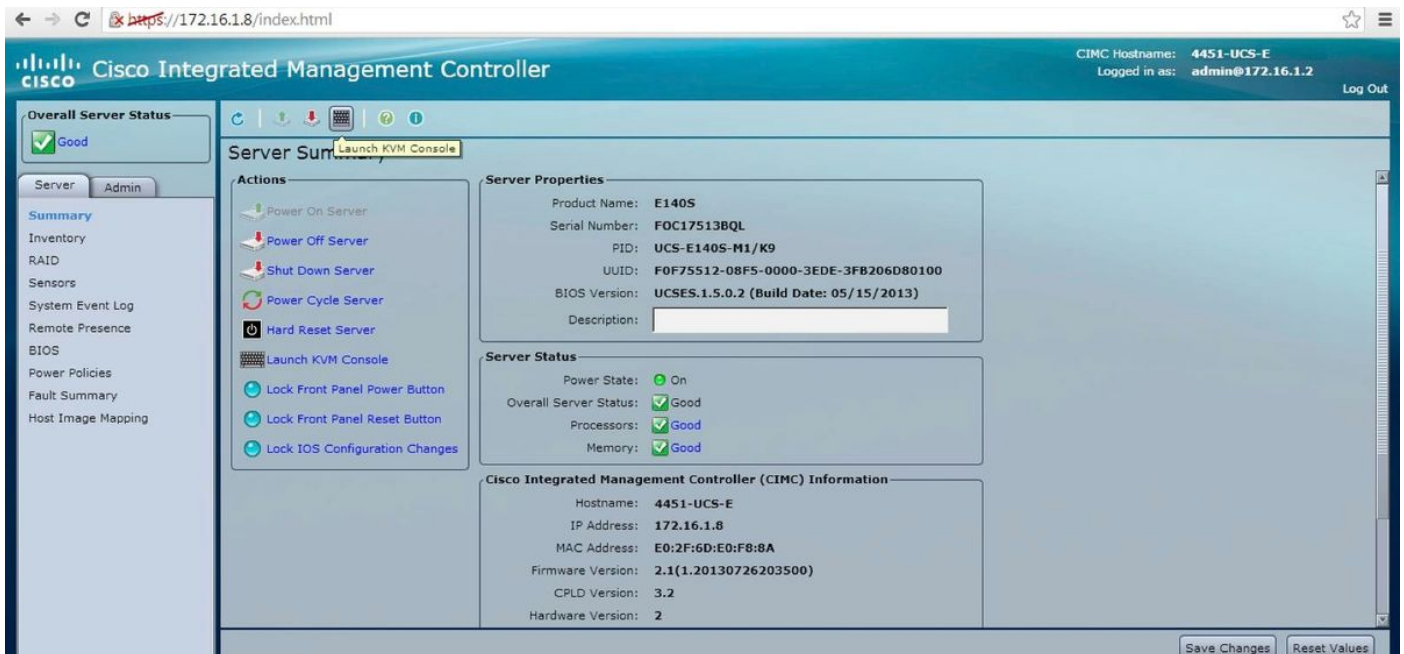
イメージに示すようにデフォルトのユーザ名とブラウザおよびパスワードからの CIMC の Web インターフェイスを起動させて下さい。デフォルトのユーザ名およびパスワードは次のとおりです:

- ユーザ名 : admin
- パスワード : <password>

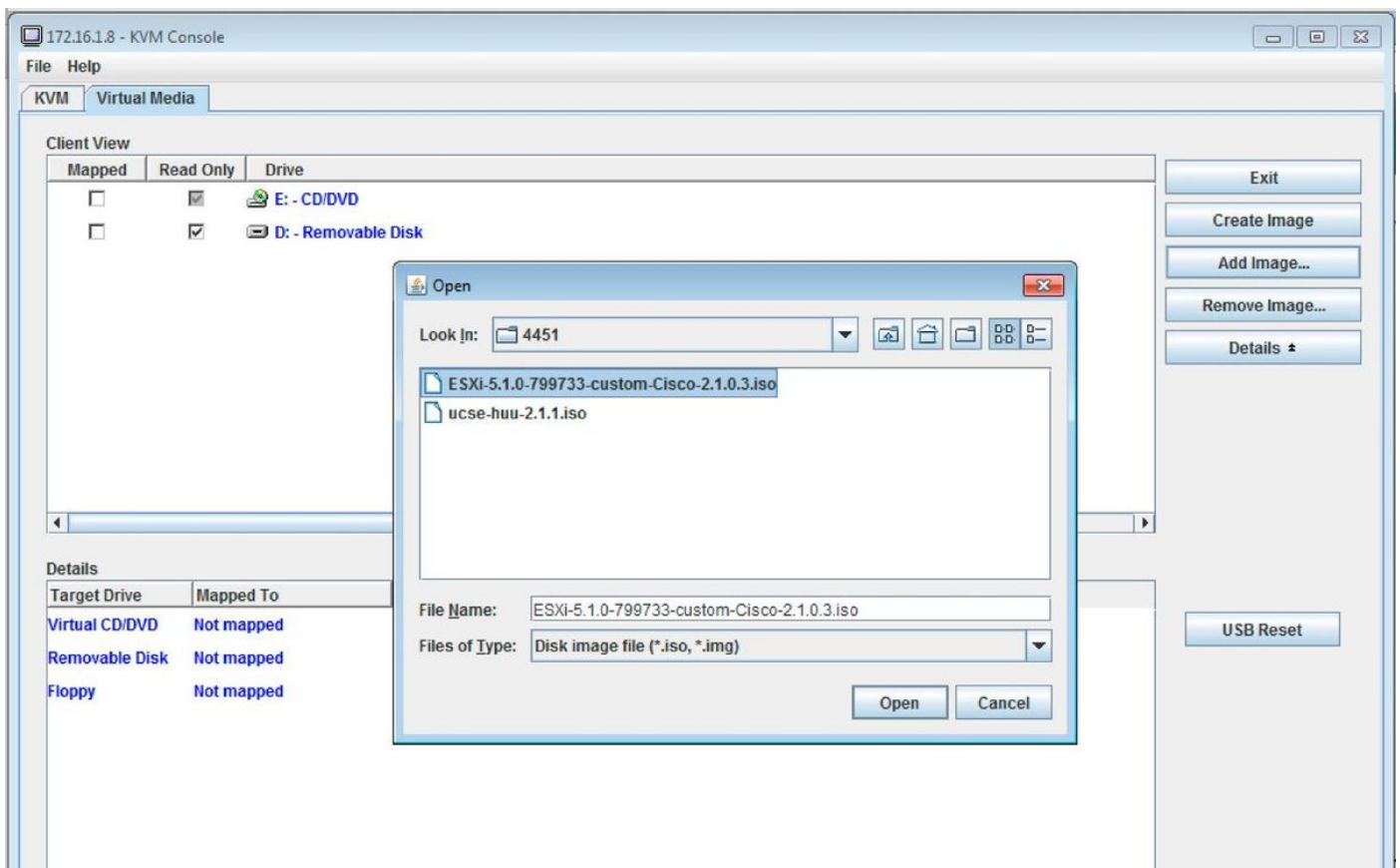


## ESXi をインストールして下さい

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。

Welcome to VMware ESXi 5.1

← https://172.16.1.10

# VMware ESXi 5.1

## Welcome

### Getting Started

If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.

- [Download vSphere Client](#)

To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

- [Download VMware vCenter](#)

If you need more help, please refer to our documentation library:

- [vSphere Documentation](#)

### For Administrators

#### vSphere Remote Command Line

The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.

- [Download the Virtual Appliance](#)
- [Download the Windows Installer \(exe\)](#)
- [Download the Linux Installer \(tar.gz\)](#)

#### Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- [Browse datastores in this host's inventory](#)

### For Developers

#### vSphere Web Services SDK

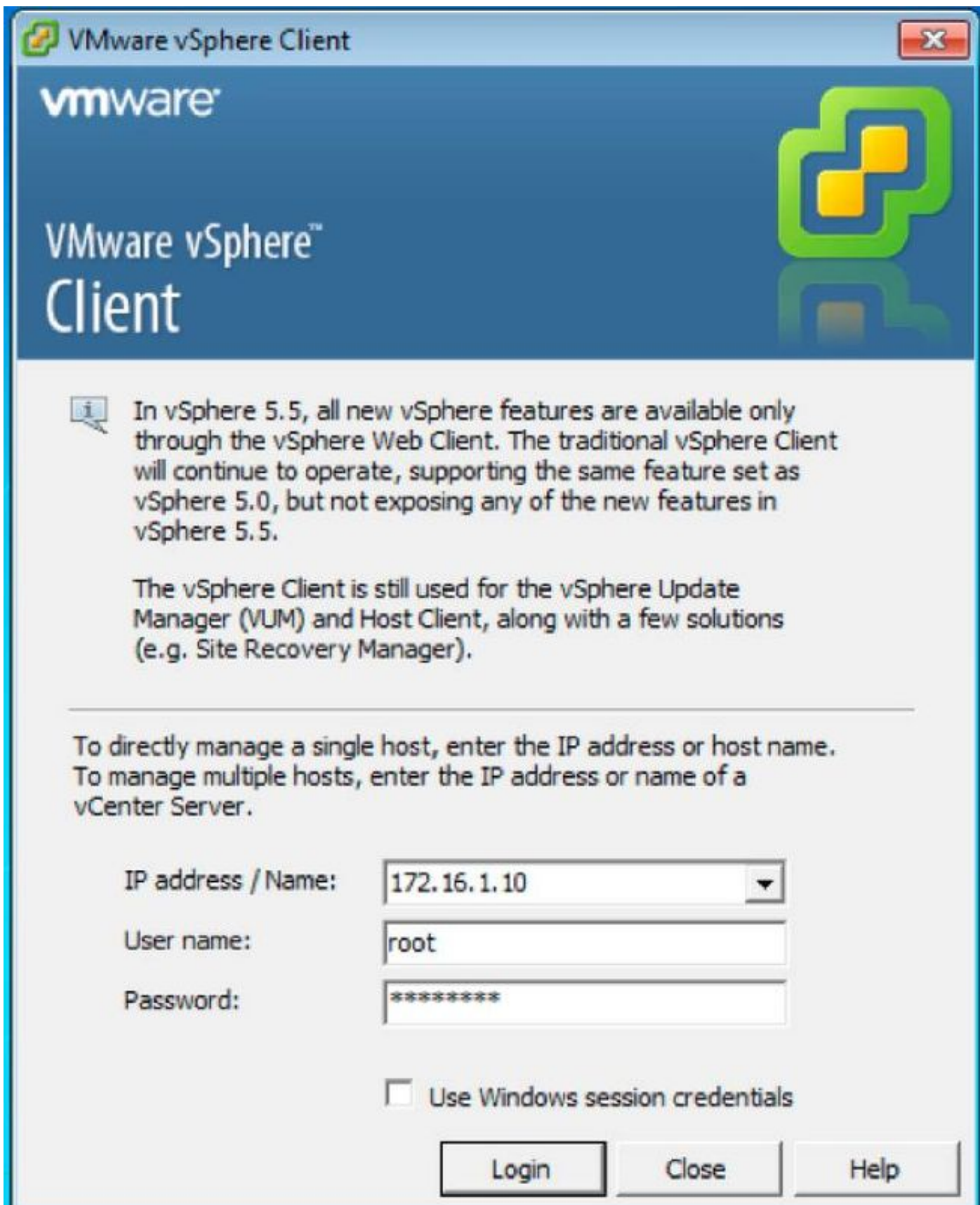
Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

- [Learn more about the Web Services SDK](#)

## 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イスです

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イスです

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。
- *vmnic3* 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。

localhost.localdomain VMware ESXi, 5.1.0, 799733

Getting Started Summary Virtual Machines Resource Allocation Performance **Configuration** Local Users & Groups Events Permissions

**Hardware**

- Health Status
- Processors
- Memory
- Storage
- Networking**
- Storage Adapters
- Network Adapters
- Advanced Settings
- Power Management

**Software**

- Licensed Features
- Time Configuration
- DNS and Routing
- Authentication Services
- Virtual Machine Startup/Shutdown
- Virtual Machine Swapfile Location
- Security Profile
- Host Cache Configuration
- System Resource Allocation
- Agent VM Settings
- Advanced Settings

View: vSphere Standard Switch

**Networking**

Standard Switch **vSwitch0** Remove... Properties...

Virtual Machine Port Group

- VM Network
- 3 virtual machine(s)
- 4451-VMware vCenter Server Appl...
- SFS
- DC

Physical Adapters

- vmnic2 1000 Full

VMkernel Port

- Management Network
- vmk0 : 172.16.1.10
- fe80::e22f:6dff:fee0:f888

Standard Switch **vSwitch1** Remove... Properties...

Virtual Machine Port Group

- SF-Inside
- 1 virtual machine(s)
- SFS

Physical Adapters

- vmnic0 1000 Full

Standard Switch **vSwitch2** Remove... Properties...

Virtual Machine Port Group

- SF-Outside
- 1 virtual machine(s) | VLAN ID: 20
- SFS

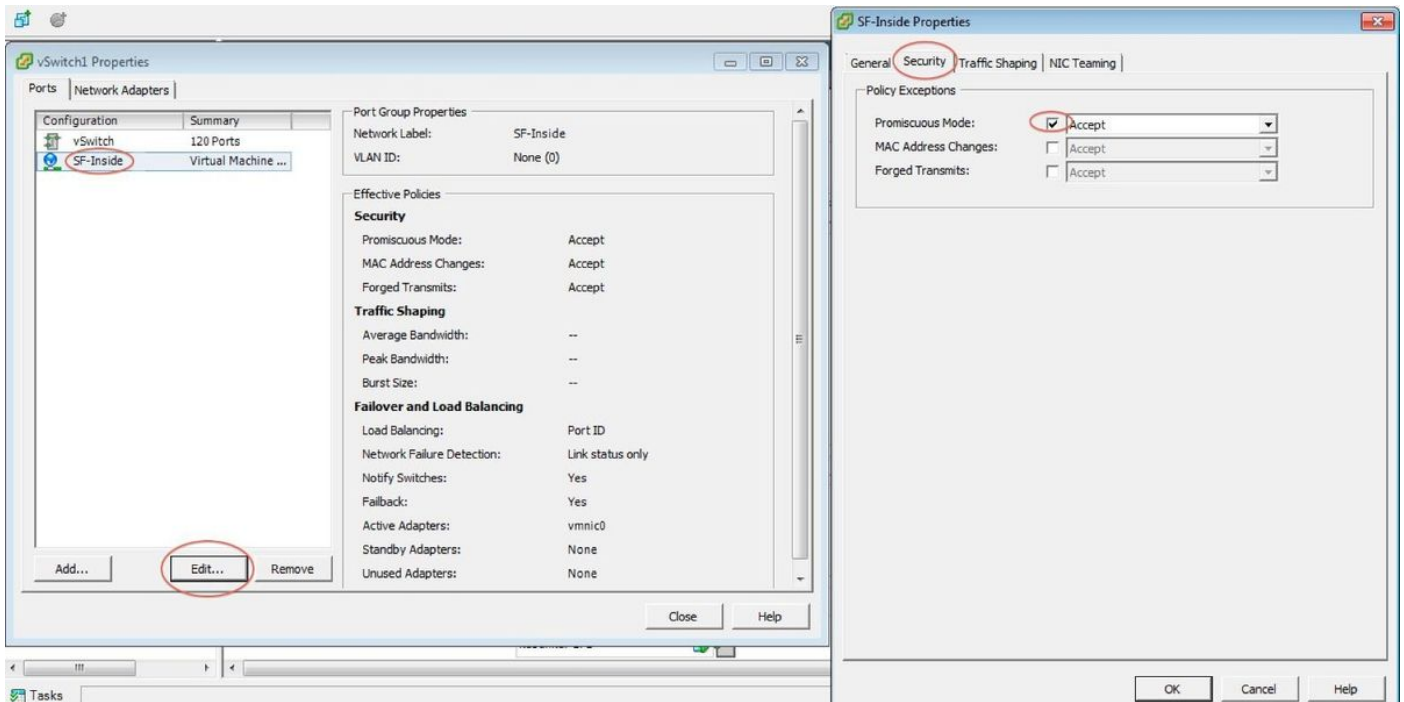
Physical Adapters

- vmnic1 1000 Full

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:

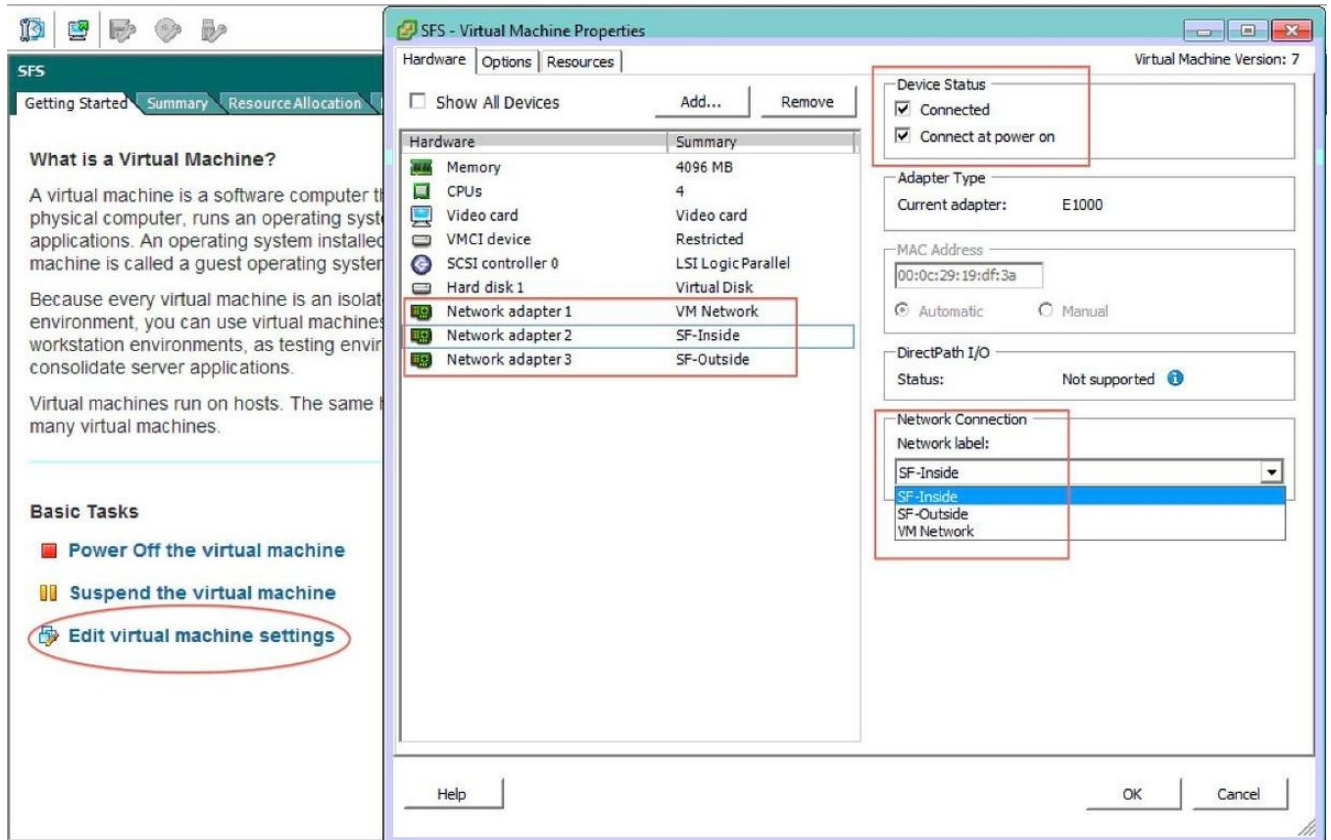
注: これが NGIPsv 資料に従って必要となることをように VLAN ID 設定される NGIPsv のための 4095 にして下さい:

[http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick\\_start/ngips\\_virtual/NGIPsv-quick/install-ngipsv.html](http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPsv-quick/install-ngipsv.html)



ESXi の vSwitch 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のイメージに示すように、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 コマンドの代わりに 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
```

## 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](#)