使用UCS-E刀片在ISR设备上配置FirePOWER服务

目录

简介

本文档介绍如何在入侵检测系统(IDS)模式下在思科统一计算系统E系列(UCS-E)刀片平台上安装和部署Cisco FirePOWER软件。本文档中介绍的配置示例是对官方用户指南的补充。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科集成多业务路由器(ISR)XE映像3.14或更高版本
- 思科集成管理控制器(CIMC)2.3版或更高版本
- Cisco FireSIGHT管理中心(FMC)5.2版或更高版本
- Cisco FirePOWER虚拟设备(NGIPSv)5.2版或更高版本
- VMware ESXi 5.0版或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

> **注意**：在将代码升级到3.14版或更高版本之前，请确保系统具有足够的内存、磁盘空间和升级许可证。请参阅示例1:将映像从 TFTP 服务器复制到 flash:从访问路由器软件升级过程Cisco文档的TFTP服务器部分了解有关代码升级的详细信息。

> **注意**：为了升级CIMC、BIOS和其他固件组件，您可以使用思科主机升级实用程序(HUU)，也可以手动升级固件组件。要了解有关固件升级的详细信息，请参阅Cisco UCS E系列服务器和Cisco UCS E系列网络计算引擎的主机升级实用程序用户指南部分的Upgrading the Firmware on Cisco UCS E系列服务器升级固件。

背景信息

本节提供有关受支持的硬件平台、许可证以及与本文档中所述组件和过程相关的限制的信息。

支持的硬件平台

本节列出G2和4000系列设备支持的硬件平台。

带UCS-E刀片的ISR G2设备

支持以下带UCS-E系列刀片的ISR G2系列设备：

产品	Platform	UCS-E型号
Cisco 2900 系列 ISR	2911	UCS-E 120/140单宽选件
	2921	UCS-E 120/140/160/180单宽或双宽选项
	2951	UCS-E 120/140/160单宽或双宽选项
Cisco 3900 系列 ISR	3925	UCS-E 120/140/160单宽和双宽选项或180双宽
	3925E	UCS-E 120/140/160单宽和双宽选项或180双宽
	3945	UCS-E 120/140/160单宽和双宽选项或180双宽
	3945E	UCS-E 120/140/160单宽和双宽选项或180双宽

带UCS-E刀片的ISR 4000设备

支持以下带UCS-E系列刀片的ISR 4000系列设备：

产品	Platform	UCS-E型号
Cisco 4400 系列 ISR	4451	UCS-E 120/140/160单宽和双宽选项或180双宽
	4431	UCS-E网络接口模块
Cisco 4300 系列 ISR	4351	UCS-E 120/140/160/180单宽和双宽选项或180双宽
	4331	UCS-E 120/140单宽选件
	4321	UCS-E网络接口模块

许可证

ISR必须具有安全K9许可证和appx许可证才能启用服务。

限制

以下是本文档中介绍的信息的两个限制：

- 不支持组播
- 每个系统仅支持4,096个网桥域接口(BDI)

BDI不支持以下功能：

- 双向转发检测(BFD)协议
- Netflow
- 服务质量 (QoS)
- 基于网络的应用识别(NBAR)或高级视频编码(AVC)
- 基于区域的防火墙(ZBF)
- 加密VPN
- 多协议标签交换（MPLS）
- 以太网点对点协议(PPPoE)

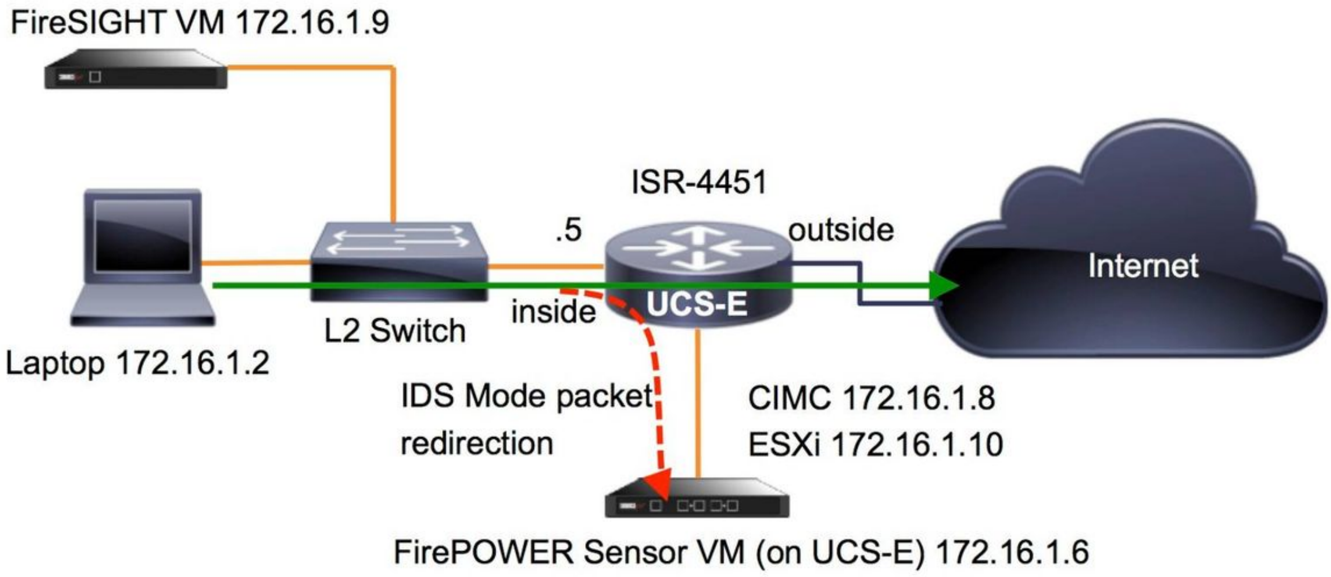
注意：对于BDI，最大传输单位(MTU)大小可以配置1,500到9,216字节之间的任意值。

配置

本节介绍如何配置与此部署相关的组件。

网络图

本文档中描述的配置使用以下网络拓扑：



UCS-E上FirePOWER服务的工作流程

以下是在UCS-E上运行的FirePOWER服务的工作流程：

1. 数据平面将流量从BDI/UCS-E接口推送出去以供检查（适用于G2和G3系列设备）。
2. Cisco IOS®-XE CLI激活数据包重定向以进行分析（所有接口或每个接口的选项）。
3. 传感器CLI设**置启**动脚本简化了配置。

配置CIMC

本节介绍如何配置CIMC。

连接到CIMC

有多种方法可连接到CIMC。在本例中，通过专用管理端口完成与CIMC的连接。确保使用以太网**电**缆将M端口（专用）连接到网络。连接后，在路由器提示符**下运行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，请运行**^a^q**。

提示 2:默认用户名为**admin**，密码为<password>。密码重置过程如下所述：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

使用以下信息完成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
```

警告：确保运行**commit**命令以保存更改。

注意：使用管理端口**时**，该模式设置为专用。

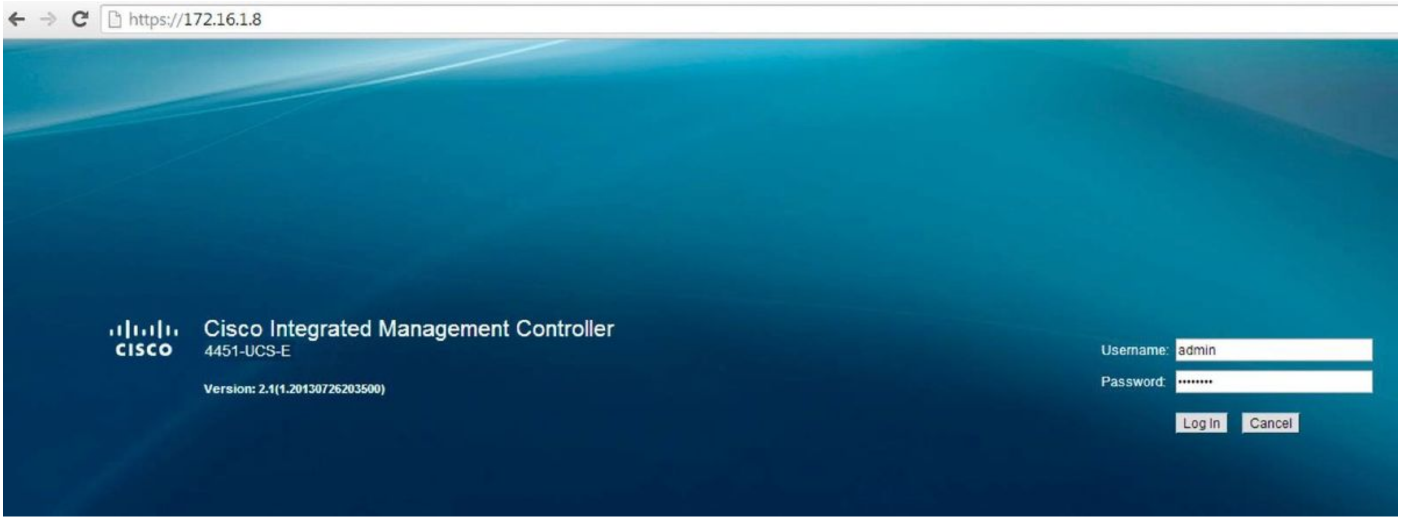
运行**show detail**命令以验证详细设置：

```
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 #
```

从浏览器启动CIMC的Web界面，其默认用户名和密码如图所示。默认用户名和密码为：

- username：**admin**

- 密码：<**密码**>

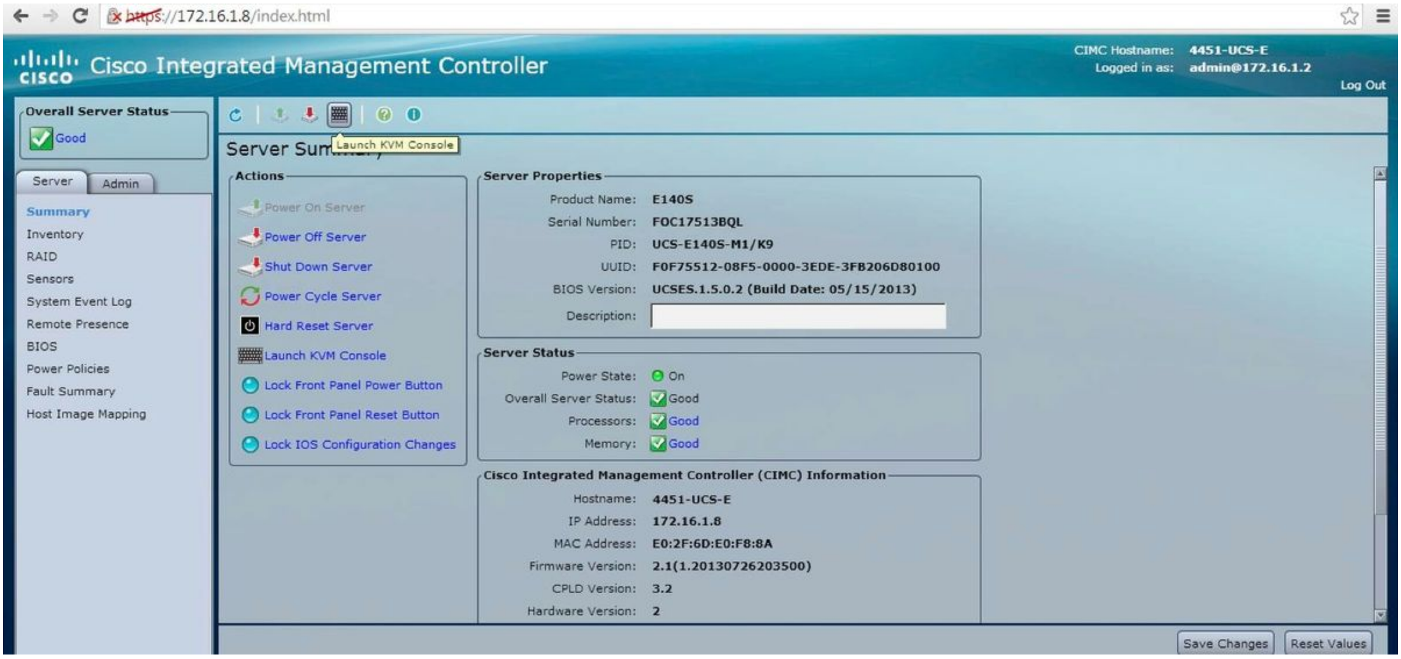

https://172.16.1.8

Cisco Integrated Management Controller
4451-UCS-E
Version: 2.1(1.20130726203500)

Username: admin
Password: ••••••••

安装ESXi

登录CIMC的用户界面后，您可以查看与此图中显示的类似页面。单击“**Launch KVM Console(启**动KVM控制台)”图**标，单击**“Add image（添加映像）”，然后将ESXi ISO映射为虚拟介质：


~~https~~://172.16.1.8/index.html

Cisco Integrated Management Controller
CIMC Hostname: 4451-UCS-E
Logged in as: admin@172.16.1.2

Overall Server Status: Good

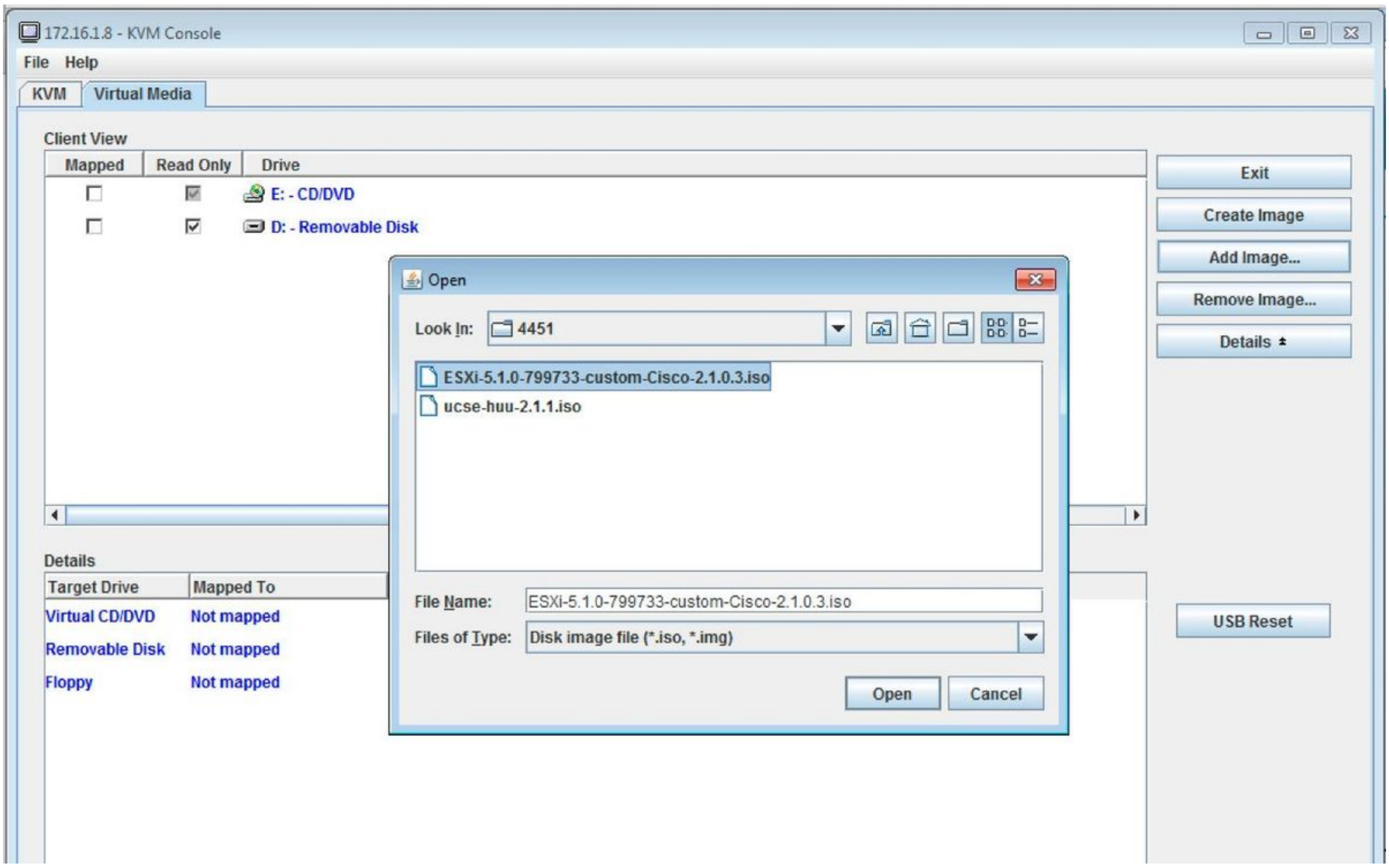
Server Summary

Server Properties
Product Name: E140S
Serial Number: FOC17513BQL
PID: UCS-E140S-M1/K9
UUID: F0F75512-08F5-0000-3EDE-3FB206D80100
BIOS Version: UCSES.1.5.0.2 (Build Date: 05/15/2013)
Description:

Server Status
Power State: On
Overall Server Status: Good
Processors: Good
Memory: Good

Cisco Integrated Management Controller (CIMC) Information
Hostname: 4451-UCS-E
IP Address: 172.16.1.8
MAC Address: E0:2F:6D:E0:F8:8A
Firmware Version: 2.1(1.20130726203500)
CPLD Version: 3.2
Hardware Version: 2

单击“**虚拟媒**体”选项卡，然后单击**“添加映**像”以映射虚拟媒体，如图所示。



Client View

Mapped	Read Only	Drive
□	☑	E: - CD/DVD
□	☑	D: - Removable Disk

Look In: 4451

ESXi-5.1.0-799733-custom-Cisco-2.1.0.3.iso
ucse-huu-2.1.1.iso

File Name: ESXi-5.1.0-799733-custom-Cisco-2.1.0.3.iso

Files of Type: Disk image file (*.iso, *.img)

Details

Target Drive	Mapped To
Virtual CD/DVD	Not mapped
Removable Disk	Not mapped
Floppy	Not mapped

映射虚拟介质后，单击CIMC主**页中的Power Cycle Server**以对UCS-E重新通电。ESXi设置从虚拟介质启动。完成ESXi安装。

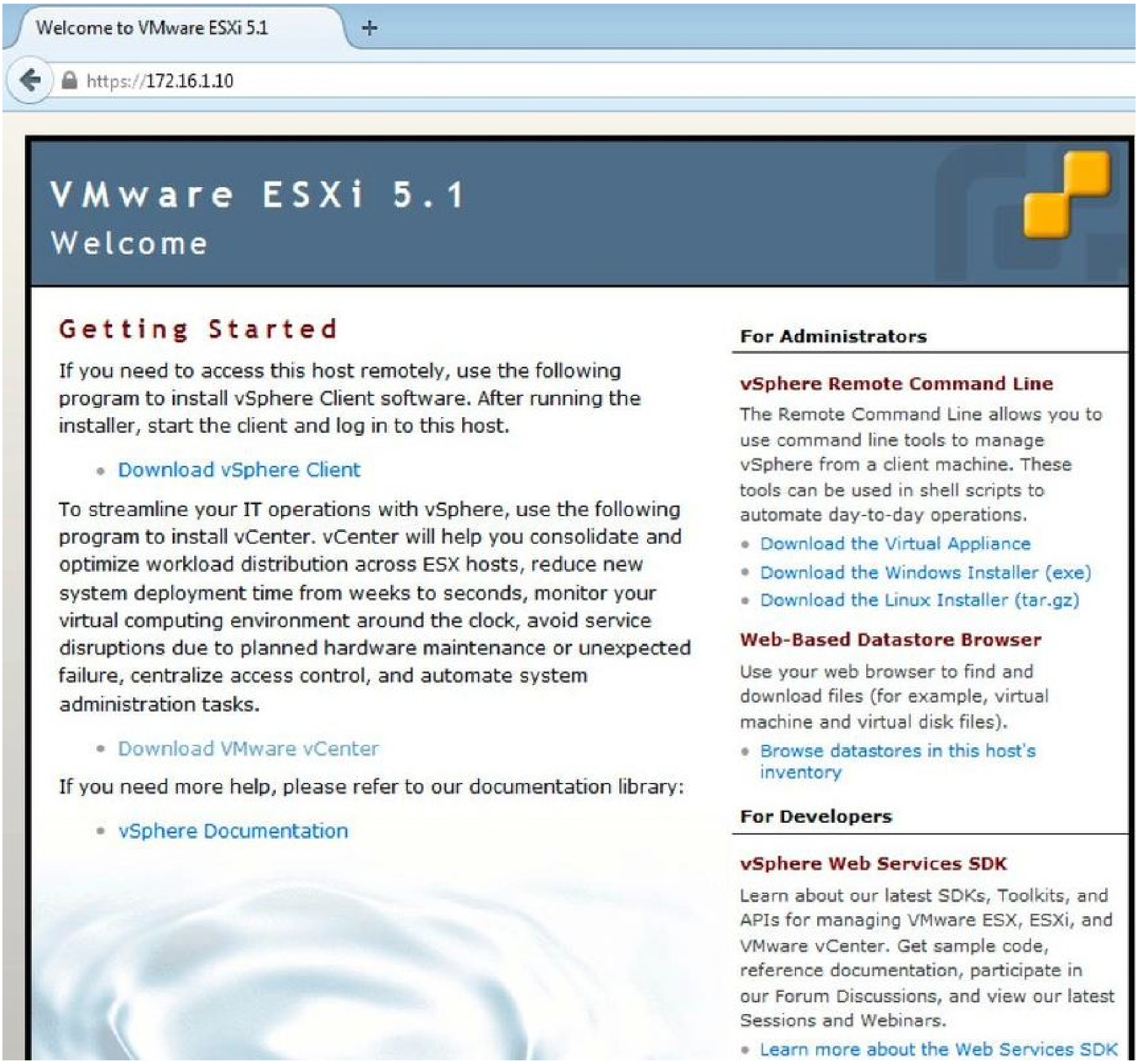
注意：记录ESXi IP地址、用户名和密码，以供将来参考。

安装vSphere客户端

本节介绍如何安装vSphere客户端。

下载vSphere客户端

启动ESXi并使用**下载VSphere客户端**链接下载vSphere客户端。将其安装到计算机上。



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

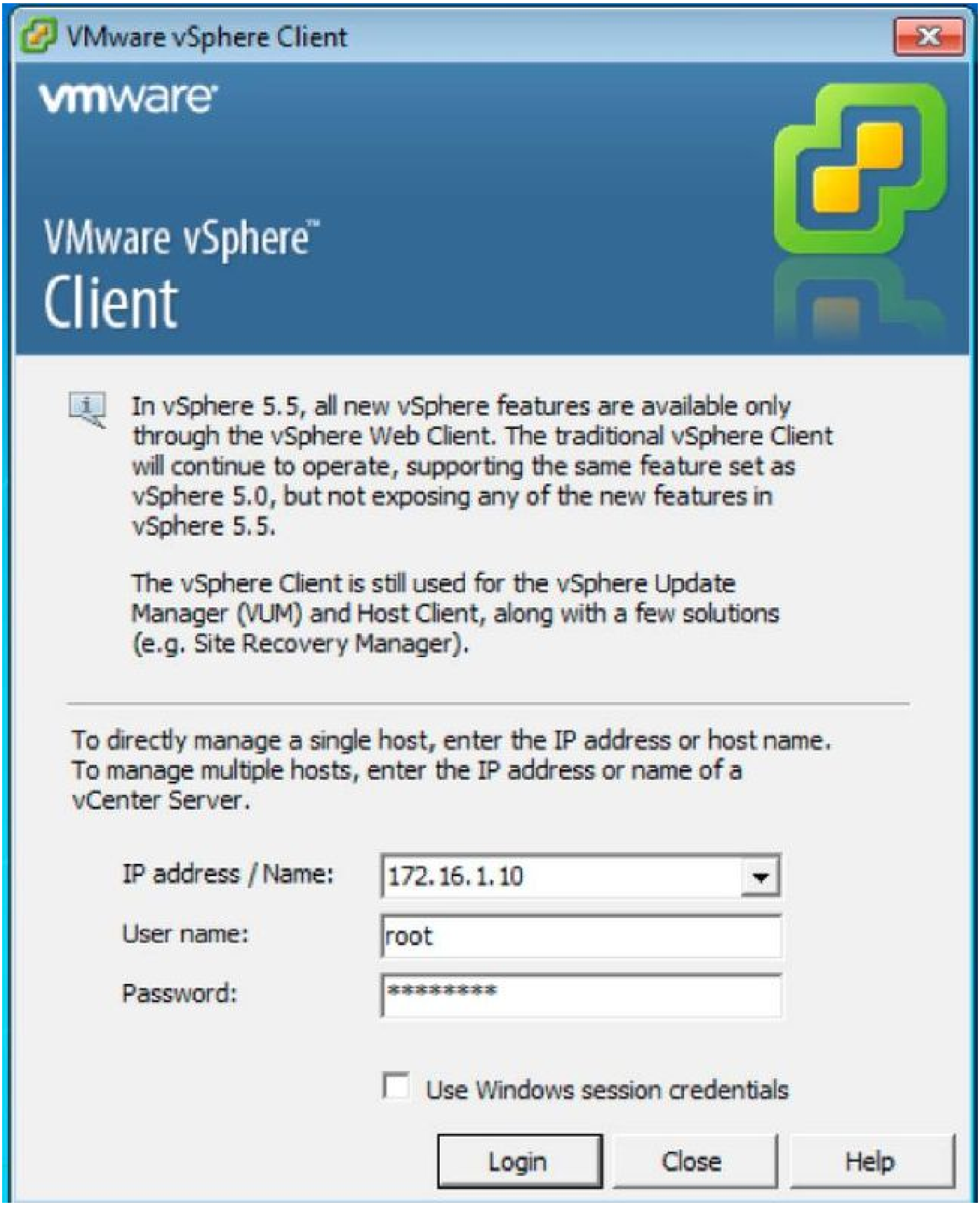
vSphere Web Services SDK

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

启动vSphere客户端

从计算机启动vSphere客户端。使用您在安装过程中创建的用户名和密码登录，如图所示：



In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5.

The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager).

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: 172.16.1.10

User name: root

Password: *********

□ Use Windows session credentials

部署FireSIGHT管理中心和FirePOWER设备

完成在VMware ESXi Cisco上部署FireSIGHT管理中心文档中描述的步骤，以在ESXi上部署FireSIGHT管理中心。

注意：用于部署FirePOWER NGIPSv设备的过程与部署管理中心的过程类似。

接口

在双宽UCS-E上，有四个接口：

- 最高MAC地址接口是前面板上的Gi3
- 第二高的MAC地址接口是前面板上的Gi2
- 最后两个显示为内部接口

在单宽UCS-E上，有三个接口：

- 最高MAC地址接口是前面板上的Gi2
- 最后两个显示为内部接口

ISR4K上的两个UCS-E接口都是中继端口。

UCS-E 120S和140S有三个网络适配器和管理端口：

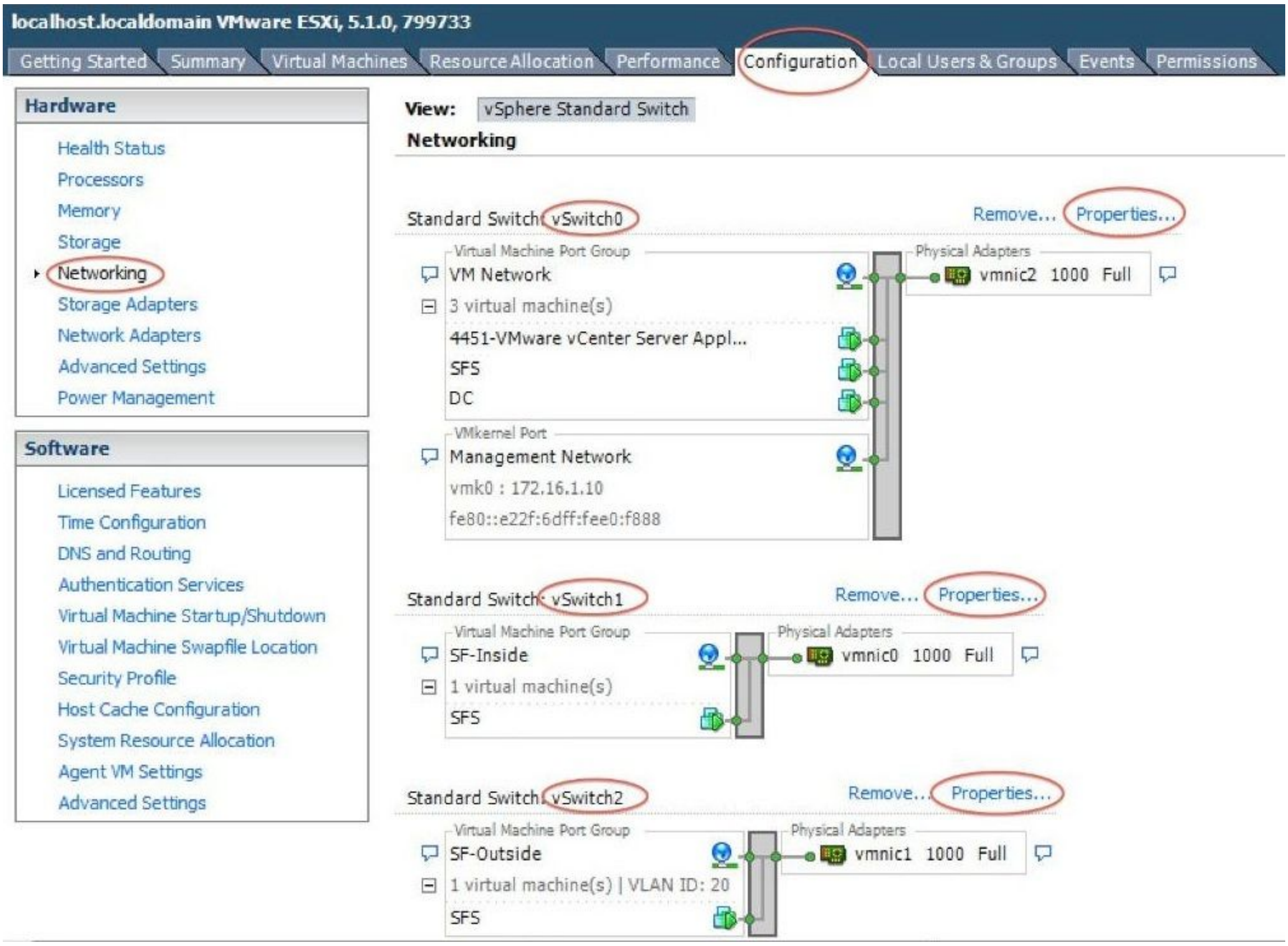
- vmnic0*映*射到路*由器背板上*的UCSEx/0/0
- vmnic1*映*射到路*由器背板上*的UCSEx/0/1
- *vmnic2*映射到UCS-E前面GE2接口
- 前面板管理(M)端口只能用于CIMC。

UCS-E 140D、160D和180D有四个网络适配器：

- vmnic0*映*射到路*由器背板上的*UCSEx/0/0。
- vmnic1*映*射到路*由器背板上的*UCSEx/0/1。
- *vmnic2*映射到UCS-E前平面GE2接口。
- *vminc3*映射到UCS-E前面GE3接口。
- 前面板管理(M)端口只能用于CIMC。

ESXi上的vSwitch接口

ESXi上的vSwitch0是ESXi、FireSIGHT管理中心和FirePOWER NGIPSv设备与网络通信的管理接口。单击vSwitch1(SF-Inside)和vSwitch2(SF-Outside)的**Properties**以进行任何更改。



View: vSphere Standard Switch

Networking

Standard Switch: vSwitch0

Virtual Machine Port Group: VM Network — 3 virtual machine(s): 4451-VMware vCenter Server Appl..., SFS, DC

VMkernel Port: Management Network — vmk0 : 172.16.1.10, fe80::e22f:6dff:fee0:f888

Physical Adapters: vmnic2 1000 Full

Standard Switch: vSwitch1

Virtual Machine Port Group: SF-Inside — 1 virtual machine(s): SFS

Physical Adapters: vmnic0 1000 Full

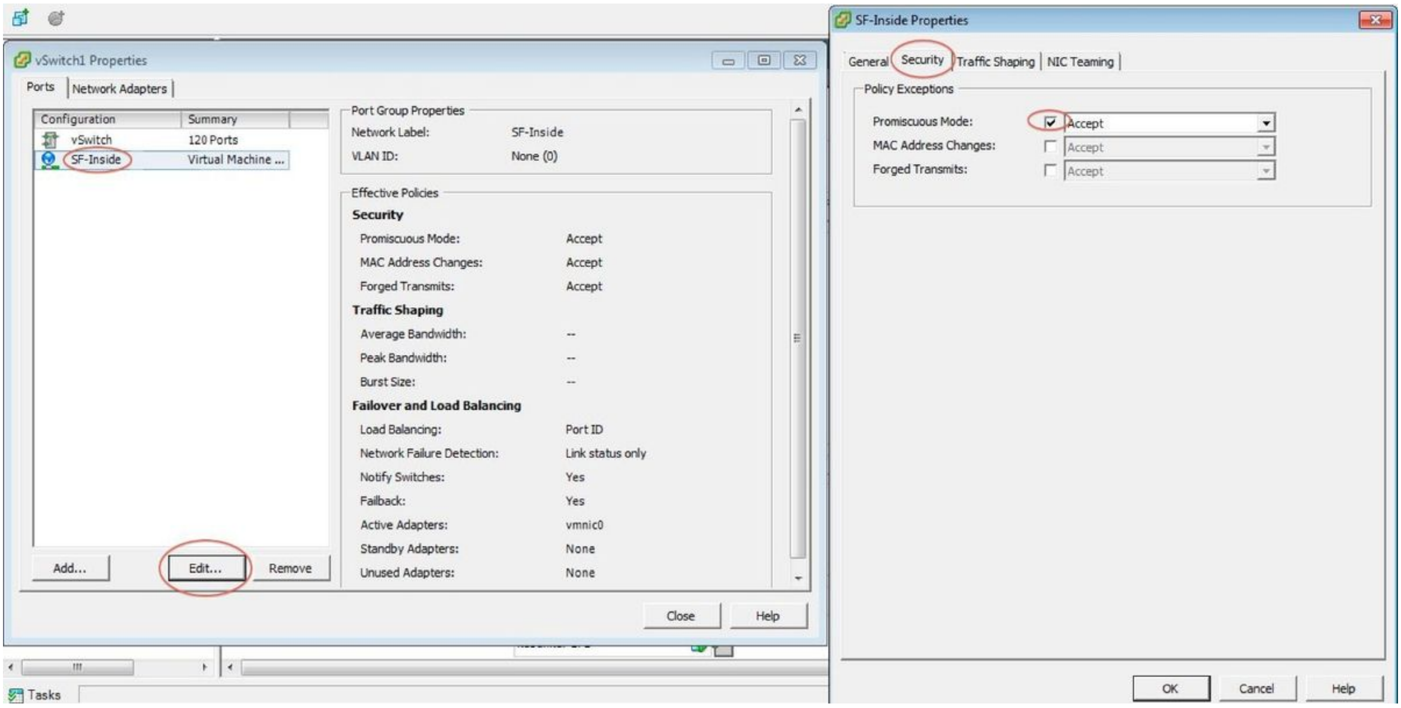
Standard Switch: vSwitch2

Virtual Machine Port Group: SF-Outside — 1 virtual machine(s) | VLAN ID: 20: SFS

Physical Adapters: vmnic1 1000 Full

下图显示vSwitch1的属性（您必须完成vSwitch2的相同步骤）：

注意：确保NGIPSv的VLAN ID配置为4095，根据NGIPSv文档，这是必需的：http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



Configuration	Summary
vSwitch	120 Ports
SF-Inside	Virtual Machine ...

Port Group Properties

Network Label: SF-Inside

VLAN ID: None (0)

Effective Policies

Security

Promiscuous Mode: Accept

MAC Address Changes: Accept

Forged Transmits: Accept

Traffic Shaping

Average Bandwidth: --

Peak Bandwidth: --

Burst Size: --

Failover and Load Balancing

Load Balancing: Port ID

Network Failure Detection: Link status only

Notify Switches: Yes

Failback: Yes

Active Adapters: vmnic0

Standby Adapters: None

Unused Adapters: None

Policy Exceptions

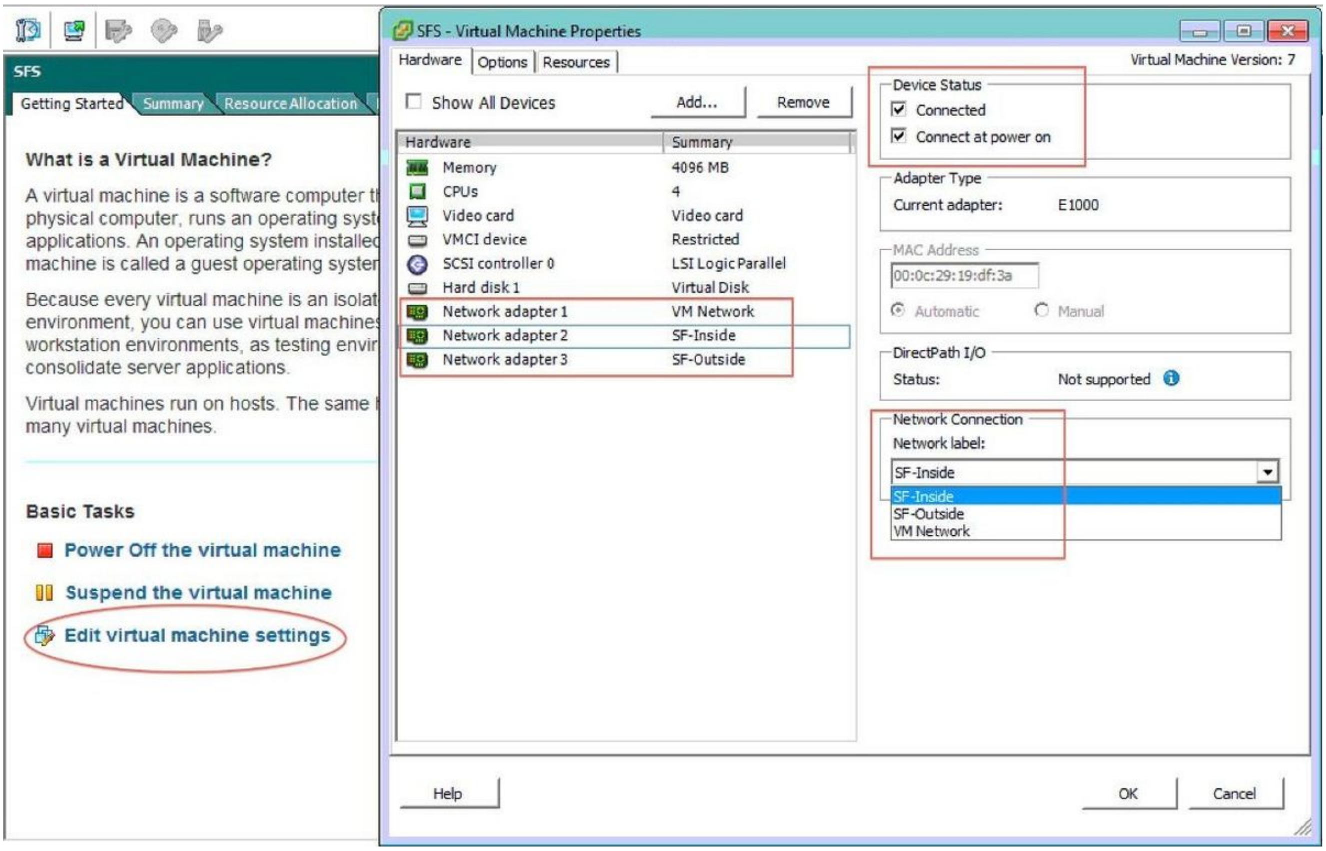
Promiscuous Mode: ☑ Accept

MAC Address Changes: □ Accept

Forged Transmits: □ Accept

ESXi上的vSwitch配置已完成。现在，您必须验证接口设置：

1. 导航至FirePOWER设备的虚拟机。
2. 单击“**编辑虚拟机设置**”。
3. 检验所有三个网络适配器。
4. 确保正确选择它们，如下图所示：



What is a Virtual Machine?

A virtual machine is a software computer t
physical computer, runs an operating syst
applications. An operating system installe
machine is called a guest operating syster

Because every virtual machine is an isolat
environment, you can use virtual machine
workstation environments, as testing envir
consolidate server applications.

Virtual machines run on hosts. The same
many virtual machines.

Basic Tasks

- Power Off the virtual machine
- Suspend the virtual machine
- Edit virtual machine settings

Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	SF-Inside
Network adapter 3	SF-Outside

Device Status
☑ Connected
☑ Connect at power on

Adapter Type
Current adapter: E1000

MAC Address
00:0c:29:19:df:3a
● Automatic ○ Manual

DirectPath I/O
Status: Not supported

Network Connection
Network label:
SF-Inside
SF-Inside
SF-Outside
VM Network

使用FireSIGHT管理中心注册FirePOWER设备

完成思科文档中描述的步骤，以便在FireSIGHT管理中心注册FirePOWER设备。

重定向和验证流量

使用本部分可确认配置能否正常运行。

本节介绍如何重定向流量以及如何验证数据包。

在UCS-E上将流量从ISR重定向到传感器

使用此信息以重定向流量：

```
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
```

> **注意：**如果当前运行3.16.1版或更高版本，请运行**utd engine advanced**命令，而不是**utd**命令。

检验数据包重定向

在ISR控制台中，运行以下命令以验证数据包计数器是否增加：

```
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
```

验证

您可以运行以下**show**命令，以验证您的配置是否正常工作：

- **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**

故障排除

本部分提供了可用于对配置进行故障排除的信息。

您可以运行以下**debug**命令来排除配置故障：

- **debug platform condition feature utd controlplane**
- **debug platform condition feature utd dataplan子模式**

相关信息

- Cisco UCS E系列服务器和Cisco UCS E系列网络计算引擎2.x版入门指南
- Cisco UCS E系列服务器和Cisco UCS E系列网络计算引擎故障排除指南
- Cisco UCS E系列服务器和Cisco UCS E系列网络计算引擎2.x版入门指南 — 升级固件
- Cisco ASR 1000系列聚合服务路由器软件配置指南 — 配置网桥域接口
- Cisco UCS E系列服务器和Cisco UCS E系列网络计算引擎的主机升级实用程序用户指南 — 升级Cisco UCS E系列服务器上的固件
- 技术支持和文档 - Cisco Systems