



Cisco UCS Manager VM-FEX for VMware CLI Configuration Guide, Release 3.0

First Published: November 20, 2015

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface vii

Audience vii

Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1

Introduction 1

Overview of Virtualization 1

Overview of Cisco Virtual Machine Fabric Extender 1

Virtualization with a Virtual Interface Card Adapter 2

Virtualization with Network Interface Cards and Converged Network Adapters 2

VM-FEX for VMware Components and Requirements 3

Hypervisor Host 3

Cisco UCS Manager 4

VMware vCenter 6

Modes of Operation 6

Standard Mode 7

High-Performance Mode 7

Configuring VM-FEX for VMware 8

CHAPTER 2

Configuring a Service Profile with VM-FEX 11

Modifying the VMwarePassThrough Ethernet Adapter Policy 11

Configuring Dynamic vNIC Connection Policies 12

Dynamic vNIC Connection Policy 12

Creating a Dynamic vNIC Connection Policy 13

Deleting a Dynamic vNIC Connection Policy 15

Viewing Dynamic vNIC Properties in a VM 15

Configuring the VM Lifecycle Policy	16
VM Lifecycle Policy	16
Configuring the VM Lifecycle Policy	17
Creating a BIOS Policy for VM-FEX in High-Performance Mode	17

CHAPTER 3

Installing the Cisco VM-FEX Driver Software Bundle	19
Cisco VM-FEX Driver Software Bundle Installation Overview	19
Cisco VM-FEX Driver Software Bundle Prerequisites	19
Installing or Upgrading the Cisco VM-FEX Driver Software Bundle Using VUM	20
Upgrading a Host to ESX or ESXi 4.0, Update 3 or to ESX or ESXi 4.1, Update 1 and the Compatible Cisco VM-FEX Driver Software Bundle	21
Upgrading a Host to ESXi 5.0 and the Compatible Cisco VM-FEX Driver Software Bundle	23
Upgrading a Host From ESXi 5.0 to ESXi 5.1 and the Compatible Cisco VM-FEX Driver Software Bundle	24
Upgrading a Host to ESXi 5.1 and the Compatible Cisco VM-FEX Driver Software Bundle	25
Installing or Upgrading the Cisco VM-FEX Driver Software Bundle on an ESX or ESXi Host	26
Uninstalling the Cisco VM-FEX Driver Software Bundle	28

CHAPTER 4

Connecting Cisco UCS Manager to VMware vCenter	31
Connecting Using the Extension Key	31
(Optional) Modifying the vCenter Extension Key	31
Exporting a vCenter Extension File from Cisco UCS Manager	32
Registering a vCenter Extension File in VMware vCenter	32
(Optional) Configuring a Certificate for VM-FEX	33
(Optional) Creating a Certificate for VM-FEX for VMware	33
(Optional) Copying a Certificate to the Fabric Interconnect	34
(Optional) Deleting a Certificate for VM-FEX for VMware	35

CHAPTER 5

Configuring Distributed Virtual Switches in Cisco UCS	37
Distributed Virtual Switches	37
Overview of Creating a DVS in Cisco UCS Manager	37
Configuring a Distributed Virtual Switch	38

Managing Distributed Virtual Switches 40

Adding a Folder to a vCenter 40

Adding a Datacenter to a vCenter 40

Adding a Folder to a Datacenter 41

Deleting a Folder from a vCenter 42

Deleting a Datacenter from vCenter 43

Deleting a Folder from a Datacenter 44

CHAPTER 6

Configuring Port Profiles 45

Port Profiles 45

Creating a Port Profile 46

Deleting a Port Profile 47

Adding a Named VLAN to a Port Profile 48

Deleting a Named VLAN from a Port Profile 49

Port Profile Clients 49

Adding a Port Profile Client to a Port Profile 50

Deleting a Port Profile Client from a Port Profile 51

CHAPTER 7

Managing Pending Deletions of Distributed Virtual Switches 53

Pending Deletions of Distributed Virtual Switches 53

Viewing Pending Deletions 54

Viewing Properties for a Pending Deletion 54

Changing Properties for a Pending Deletion 55

Deleting a Pending Deletion 56



Preface

- [Audience, page vii](#)
- [Conventions, page vii](#)
- [Related Documentation, page ix](#)
- [Obtaining Documentation and Submitting a Service Request, page ix](#)

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in this font . Main titles such as window, dialog box, and wizard titles appear in this font .
Document titles	Document titles appear in <i>this font</i> .
TUI elements	In a Text-based User Interface, text the system displays appears in <code>this font</code> .
System output	Terminal sessions and information that the system displays appear in <code>this font</code> .

Text Type	Indication
CLI commands	CLI command keywords appear in this font . Variables in a CLI command appear in <i>this font</i> .
[]	Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

**Tip**

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

**Caution**

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: <http://www.cisco.com/go/unifiedcomputing/c-series-doc>.

VM-FEX for VMware Documentation

The following documentation is available for Cisco Virtual Machine Fabric Extender (VM-FEX) for VMware:

- Roadmap that lists all documentation for Cisco Unified Computing System (Cisco UCS) at the following URL: <http://www.cisco.com/go/unifiedcomputing/b-series-doc>
- The Unify Virtual and Physical Networking with Cisco Virtual Interface Card White Paper
- The Cisco Unified Computing System with Cisco VM-FEX and VMware VMDirectPath2 Deployment Guide

Other Documentation Resources

An ISO file containing all B and C-Series documents is available at the following URL: <http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821>. From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

Follow [Cisco UCS Docs on Twitter](#) to receive document update notifications.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly [What's New in Cisco Product Documentation](#), which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Follow [Cisco UCS Docs on Twitter](#) to receive document update notifications.



Introduction

This chapter includes the following sections:

- [Overview of Virtualization, page 1](#)
- [Overview of Cisco Virtual Machine Fabric Extender, page 1](#)
- [Virtualization with a Virtual Interface Card Adapter, page 2](#)
- [Virtualization with Network Interface Cards and Converged Network Adapters, page 2](#)
- [VM-FEX for VMware Components and Requirements, page 3](#)
- [Modes of Operation, page 6](#)
- [Configuring VM-FEX for VMware, page 8](#)

Overview of Virtualization

Virtualization allows you to create multiple Virtual Machines (VMs) to run in isolation, side by side on the same physical machine.

Each virtual machine has its own set of virtual hardware (RAM, CPU, NIC) upon which an operating system and fully configured applications are loaded. The operating system sees a consistent, normalized set of hardware regardless of the actual physical hardware components.

In a virtual machine, both hardware and software are encapsulated in a single file for rapid provisioning and moving between physical servers. You can move a virtual machine, within seconds, from one physical server to another for zero-downtime maintenance and continuous workload consolidation.

The virtual hardware makes it possible for many servers, each running in an independent virtual machine, to run on a single physical server. The advantages of virtualization include better use of computing resources, greater server density, and seamless server migration.

Overview of Cisco Virtual Machine Fabric Extender

A virtualized server implementation consists of one or more VMs that run as guests on a single physical server. The guest VMs are hosted and managed by a software layer called the hypervisor or virtual machine manager

(VMM). Typically, the hypervisor presents a virtual network interface to each VM and performs Layer 2 switching of traffic from a VM to other local VMs or to another interface to the external network.

Working with a Cisco virtual interface card (VIC) adapter, the Cisco Virtual Machine Fabric Extender (VM-FEX) bypasses software-based switching of VM traffic by the hypervisor for external hardware-based switching in the fabric interconnect. This method reduces the load on the server CPU, provides faster switching, and enables you to apply a rich set of network management features to local and remote traffic.

VM-FEX extends the IEEE 802.1Qbh port extender architecture to the VMs by providing each VM interface with a virtual Peripheral Component Interconnect Express (PCIe) device and a virtual port on a switch. This solution allows precise rate limiting and quality of service (QoS) guarantees on the VM interface.

Virtualization with a Virtual Interface Card Adapter

A Cisco VIC adapter is a converged network adapter (CNA) that is designed for both single-OS and VM-based deployments. The VIC adapter supports static or dynamic virtualized interfaces, which includes up to 128 virtual network interface cards (vNICs).

VIC adapters support VM-FEX to provide hardware-based switching of traffic to and from virtual machine interfaces.



Note

All models of the Cisco VICs, including **gen2**, support VM-FEX in the high performance mode as long as you are running ESXi 5.0 or higher on the hypervisor host.

In a VMware environment, VM-FEX supports the standard VMware integration with VMware ESX hypervisors installed on the server and all virtual machine management performed through the VMware vCenter.

Virtualization with Network Interface Cards and Converged Network Adapters

Network interface card (NIC) and converged network adapters support virtualized environments with the standard VMware integration with ESX installed on the server and all virtual machine management performed through the VC.

Portability of Virtual Machines

If you implement service profiles you retain the ability to easily move a server identity from one server to another. After you image the new server, the ESX treats that server as if it were the original.

Communication between Virtual Machines on the Same Server

These adapters implement the standard communications between virtual machines on the same server. If an ESX host includes multiple virtual machines, all communications must go through the virtual switch on the server.

If the system uses the native VMware drivers, the virtual switch is out of the network administrator's domain and is not subject to any network policies. As a result, for example, QoS policies on the network are not applied to any data packets traveling from VM1 to VM2 through the virtual switch.

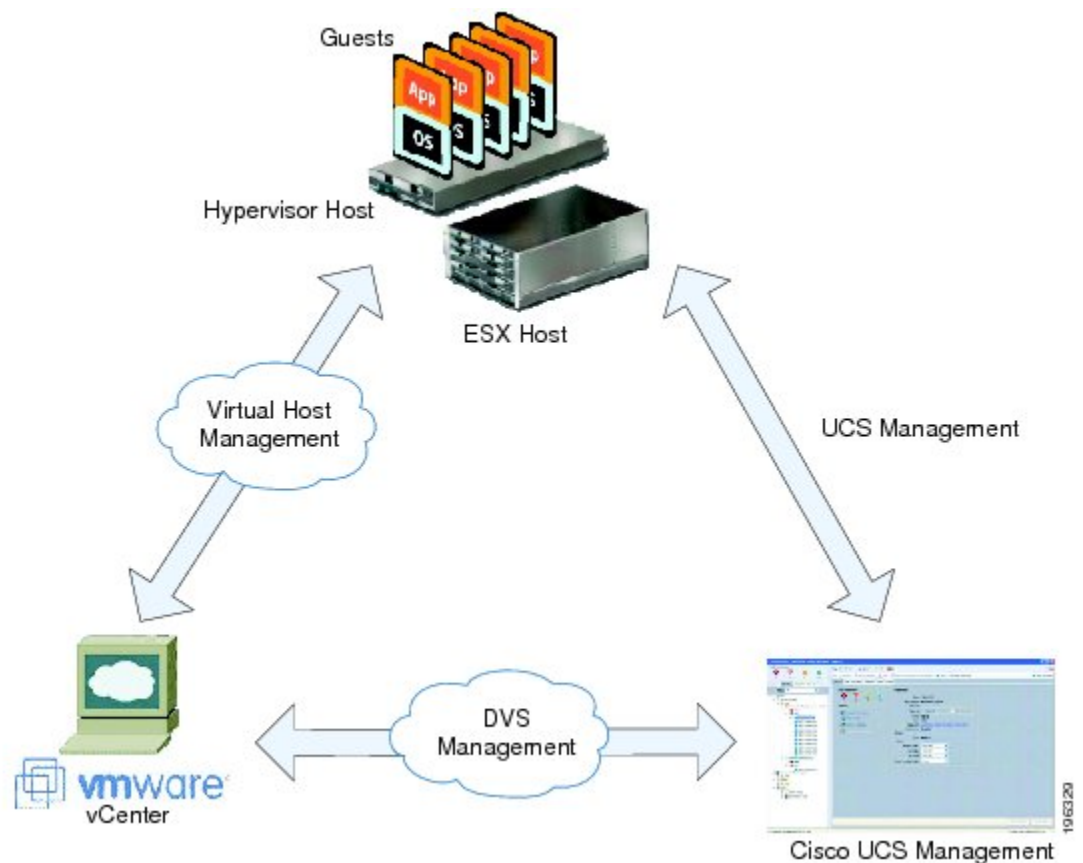
If the system includes another virtual switch, such as the Nexus 1000, that virtual switch is subject to the network policies configured on that switch by the network administrator.

VM-FEX for VMware Components and Requirements

At a high level, VM-FEX for VMware requires a hypervisor host, Cisco UCS Manager, and VMware vCenter virtualization management software.

The following figure shows these three main components and the methods by which they are connected.

Figure 1: Component Connectivity for VM-FEX with VMware



These components must be configured correctly for VM-FEX for VMware to work.

Hypervisor Host

The hypervisor host has these requirements:

- You must install a Cisco UCS Virtual Interface Card in the server you intend to use as the hypervisor host. For more information about installing Cisco UCS Virtual Interface Cards, see the *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.

- You must install the correct version of VMware ESX or ESXi software on the Cisco UCS Manager host. For VM-FEX in standard mode, you must install VMware ESX version 4.0, Update 1 software or later versions.
- You must obtain the Cisco VM-FEX Driver software bundle from the Cisco **Download Software** page:
 - For B-Series from, <http://software.cisco.com/download/navigator.html>. Select **Downloads Home > Products > Servers - Unified Computing > Cisco UCS B-Series Blade Server Software** and click **Unified Computing Systems (UCS) Drivers**. From this page, click **Latest Releases** or **All Releases** to select the release you want, and click **Download** to download the **ISO image of UCS-related drivers**.
 - For C-Series from, <http://software.cisco.com/download/navigator.html>. Select **Downloads Home > Products > Servers - Unified Computing > Cisco UCS C-Series Rack-Mount UCS-Managed Server Software** and click **Unified Computing Systems (UCS) Drivers**. From this page, click **Latest Releases** or **All Releases** to select the release you want, and click **Download** to download the **ISO image of UCS-related drivers**.
- You must install the correct version of the Cisco VM-FEX Driver software bundle on the hypervisor host. The Cisco VM-FEX Driver software bundle that you install depends on the VMware ESX or ESXi version you have installed on the hypervisor host. For information about the compatible versions of VMware ESX software and Cisco VM-FEX Driver software bundles, see VM-FEX Software Interoperability Matrix in *Hardware and Software Interoperability Matrix for B Series Servers* at http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html.

**Note**

The VEM software bundle is also a component of another product: the Cisco Nexus 1000V switch. Do not be concerned if you see references to this product during the installation of the VEM bundle. This reference is cosmetic only and does not affect the outcome of the installation and implementation of VM-FEX.

Cisco UCS Manager

VM-FEX for VMware-Related Policies

You must modify or create several policies in order for VM-FEX for VMware to function optimally:

- VMwarePassThrough Ethernet Adapter Policy (high-performance mode only)
- Dynamic vNIC Connection Policies
- BIOS Policy (high-performance mode only)
- VM Lifecycle Policy

Extension File for Communicating with VMware vCenter

For Cisco UCS domains that use VIC adapters to implement VM-FEX, you must create and install an extension file to establish the relationship and communications between Cisco UCS Manager and VMware vCenter. This extension file is an XML file that contains an extension key and public secure sockets layer (SSL) certificate.

**Important**

You cannot change an extension key that is being used by a DVS or an external virtualization manager. If you want to use a custom extension key, we recommend that you create and register the custom key before you create the DVS in Cisco UCS Manager to avoid any possibility of having to delete and recreate the associated DVS.

Extension Key

Cisco UCS and VMware vCenter must be connected for management integration and network communication with the host. To accomplish this connectivity, Cisco UCS provides an extension key that represents the Cisco UCS identity. The extension key must be registered with the external virtualization manager before the Cisco UCS domain can be acknowledged and management and network connectivity can be established.

SSL Certificate

Cisco UCS Manager generates a default, self-signed SSL certificate to support communication with a VMware vCenter. You can also create your own custom certificate to communicate with multiple VMware vCenters. When you create a custom certificate, Cisco UCS Manager recreates the extension files to include the new certificate. If you subsequently delete the custom certificate, Cisco UCS Manager recreates the extension files to include the default, self-signed SSL certificate.

To create a custom certificate, you must obtain and copy an external certificate into Cisco UCS and then create a certificate for VM-FEX that uses the certificate you copied into Cisco UCS.

Distributed Virtual Switches (DVSes)

The Cisco UCS distributed virtual switch (DVS) is a software-based virtual switch that runs along side the vSwitch in the ESX hypervisor and can be distributed across multiple ESX hosts. Unlike the vSwitch, which uses its own local port configuration, a DVS that is associated with multiple ESX hosts uses the same port configuration across all ESX hosts.

After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the VM-FEX for VMware implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.

Port Profiles

Port profiles contain the properties and settings that you can use to configure virtual interfaces in Cisco UCS for VM-FEX. The port profiles are created and administered in Cisco UCS Manager. After a port profile is created, assigned to, and actively used by one or more DVSes, any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSes.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to VMware vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile are visible in VMware vCenter. You must configure at least one port profile client for a port profile if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Port Profile Clients

The port profile client determines the DVSes to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSes in the VMware vCenter. However, you

can configure the client to apply the port profile to all DVSEs in a specific datacenter or datacenter folder or only to one DVS.

VMware vCenter

You need VMware vCenter (vCenter Server and vSphere Client) for VM-FEX for VMware. The VMware vCenter must meet the following requirements:

- The Windows-based machine that you install VMware vCenter on must have network connectivity to the Cisco UCS management port and to the uplink Ethernet port(s) being used by the ESX host. The management port connectivity is used for management plane integration between VMware vCenter and Cisco UCS Manager; the uplink Ethernet port connectivity is used for communication between VMware vCenter and the ESX host.



Note The HTTP and HTTPS ports (normally TCP 80 and 443) must not be blocked between vCenter and the Cisco UCS domain.

- A VMware vCenter extension key provided by Cisco UCS Manager must be registered with VMware vCenter before VMware vCenter acknowledges the Cisco UCS domain.



Note

VMware vCenter Server Appliance (VCSA) is not supported.

In addition, you must configure VMware vCenter with the following parameters:

- A datacenter.
- A distributed virtual switch (DVS).
- ESX hosts added to the DVS and configured to migrate to pass-through switching PTS/DVS.
- For each Cisco VIC adapter, two static vNICs (one for each fabric) added to the DVS.
- Virtual machines (VMs) required for the VMs on the server.
- (For VMware vMotion) Hosts with common shared storage (datastore) that are properly configured for vMotion.
- (For VM-FEX in high-performance mode) All guest memory on the VMs must be reserved.
- (For VM-FEX in high-performance mode) The port profiles and VMwarePassThrough Ethernet adapter policy that you have previously configured in Cisco UCS Manager must be specified.

For information about how to configure these required components in VMware vCenter, see the VMware product documentation.

Modes of Operation

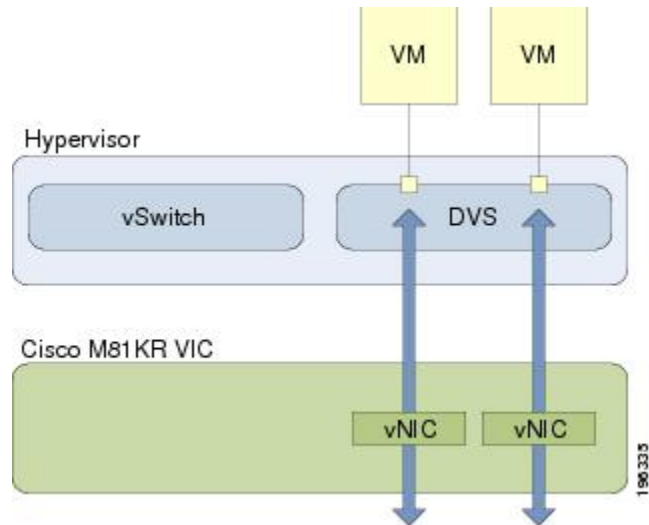
VM-FEX ports can operate in standard mode or high-performance mode.

Standard Mode

In standard mode, traffic to and from a virtual machine passes through the distributed virtual switch (DVS) and the hypervisor.

The following figure shows the traffic paths taken by VM traffic on a Cisco UCS server with a VIC adapter that has VM-FEX ports in standard mode.

Figure 2: Traffic Paths for VM Traffic with VM-FEX



High-Performance Mode

In high-performance mode, traffic to and from a virtual machine (VM) bypasses the DVS and hypervisor. Traffic travels directly between VMs and the virtual interface card (VIC) adapter.

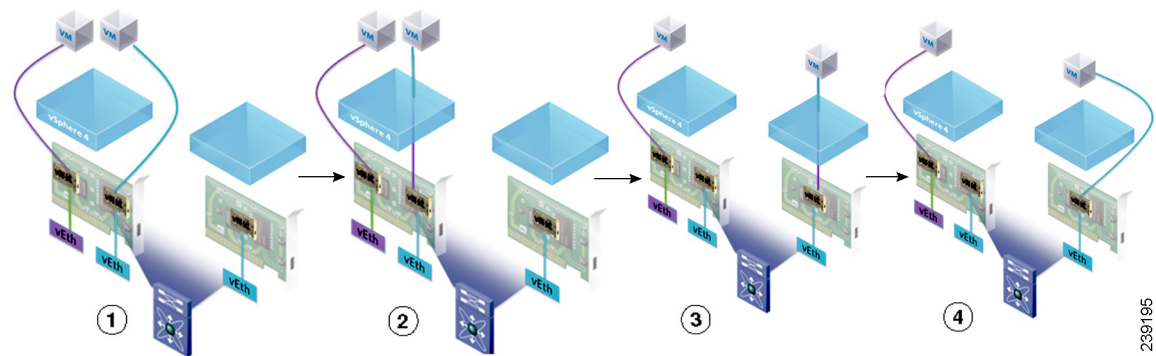
The benefits of high-performance mode are as follows:

- Increases I/O performance and throughput.
- Decreases I/O latency.
- Improves CPU utilization for virtualized I/O-intensive applications.

With VMware, high-performance mode also supports vMotion. During vMotion, the hypervisor reconfigures links in high-performance mode to be in standard mode, transitions the link to the new hypervisor, and then

reconfigures the link to be in high-performance mode. The following figure shows how VM-FEX operates in high-performance mode with vMotion.

Figure 3: VM-FEX in High-Performance Mode with vMotion



- 1 Two VMs are attached to a VIC in high-performance mode.
- 2 VMotion begins on one VM. This VM transitions to standard mode.
- 3 The VM migrates to the other host, and standard mode is established.
- 4 The VM transitions back to high-performance mode.

Configuring VM-FEX for VMware

Procedure

	Command or Action	Purpose
Step 1	Configure a Service Profile for VM-FEX for VMware.	<p>You must modify or create several policies in order for VM-FEX for VMware to function optimally:</p> <ul style="list-style-type: none"> • VMwarePassThrough Ethernet Adapter Policy (high-performance mode only) • Dynamic vNIC Connection Policies • BIOS Policy (high-performance mode only) • VM Lifecycle Policy <p>For more information, see Configuring a Service Profile with VM-FEX, on page 11.</p>
Step 2	Configure the installation of the Cisco VM-FEX Driver software bundle on the hypervisor host.	<p>You must configure the VMware ESX host and install the Cisco VM-FEX Driver software bundle and a VMware vCenter for VM-FEX. For more information, see Installing the Cisco VM-FEX Driver Software Bundle and the VMware documentation.</p>

	Command or Action	Purpose
Step 3	Connect Cisco UCS Manager to VMware vCenter.	You must connect Cisco UCS Manager with VMware vCenter to manage the distributed virtual switch (DVS) in Cisco UCS Manager. For more information, see Connecting Cisco UCS Manager to VMware vCenter, on page 31 .
Step 4	In Cisco UCS Manager, define a distributed virtual switch.	You must create a distributed virtual switch (DVS) to use in place of the VMware vSwitch. For more information, see Configuring Distributed Virtual Switches in Cisco UCS, on page 37 .
Step 5	In Cisco UCS Manager, define a port profile and (optionally) create a port profile client.	You must create a port profile to define the properties and settings used to configure the virtual interfaces in the DVS. Optionally, you can also create a port profile client that defines the DVSES to which port profiles are assigned. For more information, see Configuring Port Profiles, on page 45 .



Configuring a Service Profile with VM-FEX

This chapter includes the following sections:

- [Modifying the VMwarePassThrough Ethernet Adapter Policy, page 11](#)
- [Configuring Dynamic vNIC Connection Policies, page 12](#)
- [Configuring the VM Lifecycle Policy, page 16](#)
- [Creating a BIOS Policy for VM-FEX in High-Performance Mode, page 17](#)

Modifying the VMwarePassThrough Ethernet Adapter Policy

VM-FEX in high-performance mode has a system-provided VMwarePassThrough adapter policy. Most of the default settings are sufficient. However, you might need different settings than this policy provides to accommodate your particular implementation. If you need different settings, we recommend that you create another Ethernet adapter policy with your specific settings. In particular, you might want to check the following settings to make sure that they work with your particular implementation:

- Guest OS requirements
 - Transmit queue
 - Receive queue
 - Completion queues
 - Interrupts
- Maximum number of interfaces per host.
- Maximum number of interfaces in pass-through mode per host.

**Note**

If you have VMs with two or more vCPUS and you have upgraded from earlier versions of VM-FEX for VMware to release 2.1, you need to manually modify the following parameters with the specified values:

- `wq`—Set this parameter to 4.
- `comp-queues`—Set this parameter to 8.
- `interrupts`—Set this parameter to 12.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# <code>scope org org-name</code>	Enters organization mode for the specified organization. To enter the root organization mode, enter <code>/</code> as the <i>org-name</i> .
Step 2	UCS-A /org # <code>scope eth-policy VMWarePassThru</code>	Enters organization Ethernet policy mode for the system-provided adapter policy.
Step 3	Modify the Ethernet adapter policy settings.	(Optional) For more information about configuring an Ethernet adapter policy, see the <i>Cisco UCS Manager CLI Configuration Guide</i> .

The following example shows you how to modify a system-provided Ethernet adapter policy and commit the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope eth-policy VMWarePassThru
UCS-A /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

Configuring Dynamic vNIC Connection Policies

Dynamic vNIC Connection Policy

The dynamic vNIC connection policy determines how the connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS domains that include servers with VIC adapters on which you have installed VMs and configured dynamic vNICs.

Ethernet Adapter Policy

Each dynamic vNIC connection policy includes an Ethernet adapter policy and designates the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

For VM-FEX that has all ports on a blade in standard mode, you need to use the VMware adapter policy.

For VM-FEX that has at least one port on a blade in high-performance mode, use the VMwarePassThrough adapter policy or create a custom policy. If you need to create a custom policy, the resources provisioned need to equal the resource requirements of the guest OS that needs the most resources and for which you will be using high-performance mode.

Static vNICs



Note

In a VM-FEX deployment, a VM will attach to a dynamic vNIC without any redundancy. If a server contains more than one VIC adapter, each adapter must have two static vNICs configured.

Server Migration



Note

If you migrate a server that is configured with dynamic vNICs using VMotion, the dynamic interface used by the vNICs fails and notifies you of that failure.

When the server comes back up, assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

Creating a Dynamic vNIC Connection Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A /org # create dynamic-vnic-conn-policy <i>policy-name</i>	<p>Creates the specified vNIC connection policy and enters organization vNIC connection policy mode.</p> <p>This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.</p> <p>Note Do not specify "default" as the value for the dynamic vNIC connection policy name. Cisco UCS Manager automatically resolves any empty policy references to "default". Any service profiles or service profile templates with only static vNICs defined will automatically reference the policy "default" when it is present. If you specify "default" for the dynamic vNIC connection policy name, then unexpected dynamic vNICs might be created on those service profiles or service profile templates.</p>

	Command or Action	Purpose
Step 3	UCS-A /org/dynamic-vnic-conn-policy # set desc <i>description</i>	(Optional) Provides a description for the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote). If your description includes spaces or nonalphanumeric characters, you must begin and end your description with double quotation marks. The quotation marks do not appear in the description field of any show command output.
Step 4	UCS-A /org/dynamic-vnic-conn-policy # set adapter-policy <i>policy-name</i>	Specifies the Ethernet adapter policy to use for this policy. The adapter policy must already exist.
Step 5	UCS-A /org/dynamic-vnic-conn-policy # set dynamic-eth { <i>dynamic-eth-num</i> off }	Specifies the number of dynamic vNICs to use for this policy.
Step 6	UCS-A /org/dynamic-vnic-conn-policy # set protection { protected protected-pref-a protected-pref-b }	Dynamic vNICs are always protected in Cisco UCS, but this command allows you to select a preferred fabric, if any. You can choose one of the following options: <ul style="list-style-type: none"> • protected—Cisco UCS uses whichever fabric is available. • protected-pref-a—Cisco UCS attempts to use fabric A, but fails over to fabric B if necessary. • protected-pref-b—Cisco UCS attempts to use fabric B, but fails over to fabric A if necessary.
Step 7	UCS-A /org/dynamic-vnic-conn-policy # commit-buffer	Commits the transaction.

The following example shows how to create a dynamic vNIC connection policy named MyDynVnicConnPolicy that uses the system-provided VMWarePassThru Ethernet adapter policy for 12 dynamic vNICs and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # create dynamic-vnic-conn-policy MyDynVnicConnPolicy
UCS-A /org/dynamic-vnic-conn-policy* # set adapter-policy VMWarePassThru
UCS-A /org/dynamic-vnic-conn-policy* # set desc "Dynamic vNIC for Eth policy"
UCS-A /org/dynamic-vnic-conn-policy* # set dynamic-eth 12
UCS-A /org/dynamic-vnic-conn-policy* # commit-buffer
UCS-A /org/dynamic-vnic-conn-policy #
```


Deleting a Dynamic vNIC Connection Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, enter <i>/</i> as the <i>org-name</i> .
Step 2	UCS-A /org # delete dynamic-vnic-conn-policy <i>policy-name</i>	Deletes the specified vNIC connection policy.
Step 3	UCS-A /org # commit-buffer	Commits the transaction.

The following example shows how to delete the dynamic vNIC connection policy named MyDynVnicConnPolicy and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # delete dynamic-vnic-conn-policy MyDynVnicConnPolicy
UCS-A /org* # commit-buffer
UCS-A /org #
```

Viewing Dynamic vNIC Properties in a VM

Before You Begin

The VM must be running.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # show virtual-machine	(Optional) Displays the running virtual machines.
Step 5	UCS-A /system/vm-mgmt/vmware # scope virtual-machine <i>uuid</i>	Enters command mode for the virtual machine that contains the dynamic vNIC.
Step 6	UCS-A /system/vm-mgmt/vmware/virtual-machine # show vnic [detail]	Displays the vNIC properties.

The following example shows how to display the properties of a dynamic vNIC in a VM:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # show virtual-machine
Virtual Machine:
  UUID: 420a00c8-934b-4ae3-6af5-2ce9b8bd0f44
  Service Profile: org-root/ls-PTS-ch6-7
  Server: sys/chassis-6/blade-7
  Status: Online
.
.
.
UCS-A /system/vm-mgmt/vmware # scope virtual-machine 420a08b0-cda7-9e0a-424f-01ec8653eea0
UCS-A /system/vm-mgmt/vmware/virtual-machine # show vnic detail

vNIC:
  Name: 4479
  Status: Online
  MAC Address: 00:50:56:8A:07:B5
  Profile Name: VM-mgmt
  Virtual Adapter: sys/chassis-1/blade-1/adapter-1/host-eth-9
  Vnic Dn: org-root/ls-PTS-ch1-1/ether-dynamic-prot-009
  Current Task:

UCS-A /system/vm-mgmt/vmware/virtual-machine #
```

Configuring the VM Lifecycle Policy

VM Lifecycle Policy

The VM lifecycle policy determines how long Cisco UCS Manager retains offline VMs and offline dynamic vNICs in its database. If a VM or dynamic vNIC remains offline after that period, Cisco UCS Manager deletes the object from its database.

All virtual machines (VMs) on Cisco UCS servers are managed by vCenter. Cisco UCS Manager cannot determine whether an inactive VM is temporarily shut down, has been deleted, or is in some other state that renders it inaccessible. Therefore, Cisco UCS Manager considers all inactive VMs to be in an offline state.

Cisco UCS Manager considers a dynamic vNIC to be offline when the associated VM is shut down, or the link between the fabric interconnect and the I/O module fails. On rare occasions, an internal error can also cause Cisco UCS Manager to consider a dynamic vNIC to be offline.

The default VM and dynamic vNIC retention period is 15 minutes. You can configure a retention period of between 1 minute and 7200 minutes (2 days).



Note

The VM database displayed by Cisco UCS Manager is for information and monitoring only. You cannot manage VMs through Cisco UCS Manager. If you delete a VM from the Cisco UCS Manager database, the VM is not deleted from the server or from vCenter.

Configuring the VM Lifecycle Policy

Procedure

	Command or Action	Purpose
Step 1	Switch-A# scope system	Enters system mode.
Step 2	Switch-A /system # scope vm-mgmt	Enters VM management mode.
Step 3	Switch-A /system/vm-mgmt # scope vm-life-cycle-policy	Enters VM lifecycle policy mode.
Step 4	Switch-A /system/vm-mgmt/vm-life-cycle-policy # set vmretention {minutes 1-day 1-hour 5-days}	Specifies the period of time (minutes, one day, one hour, or five days) that an offline VM is retained in the database. If a VM remains offline after that period, it is deleted from the database. The <i>minutes</i> variable can be from 1 to 7200. The default is 15 minutes.
Step 5	Switch-A /system/vm-mgmt/vm-life-cycle-policy # set vnicretention {minutes 1-day 1-hour 5-days}	Specifies the period of time (minutes, one day, one hour, or five days) that an offline dynamic vNIC is retained in the database. If a dynamic vNIC remains offline after that period, it is deleted from the database. The <i>minutes</i> variable can be from 1 to 7200. The default is 15 minutes.
Step 6	Switch-A /system/vm-mgmt/vm-life-cycle-policy # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to configure a one-day VM retention period and a one-hour vNIC retention period and commit the transaction:

```
Switch-A# scope system
Switch-A /system # scope vm-mgmt
Switch-A /system/vm-mgmt # scope vm-life-cycle-policy
Switch-A /system/vm-mgmt/vm-mgmt/vm-life-cycle-policy # set vmretention 1-day
Switch-A /system/vm-mgmt/vm-mgmt/vm-life-cycle-policy* # set vnicretention 1-hour
Switch-A /system/vm-mgmt/vm-mgmt/vm-life-cycle-policy* # commit-buffer
Switch-A /system/vm-mgmt/vm-mgmt/vm-life-cycle-policy #
```

Creating a BIOS Policy for VM-FEX in High-Performance Mode

For VM-FEX in high performance mode, you must configure specific BIOS settings.

**Note**

pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

We recommend that you name this BIOS policy as VMwarePassThru so that you can identify it as being used for VM-FEX in high-performance mode.

You must enable these specific parameters in the following BIOS settings:

- **Processor**—Enable Virtual Technology (VT) and Direct Cache Access.

**Note**

You must enable VT if you intend to run 64-bit VMs on the ESX/ESXi host. An ESX/ESXi host will not run 64-bit VMs unless VT is enabled.

- **Intel Directed IO**—Enable the following parameters:

- VT for Directed IO
- Interrupt Remap
- Coherency Support
- ATS Support
- Pass Through DMA Support

Configure the remaining BIOS settings, as appropriate.



Installing the Cisco VM-FEX Driver Software Bundle

This chapter includes the following sections:

- [Cisco VM-FEX Driver Software Bundle Installation Overview, page 19](#)
- [Cisco VM-FEX Driver Software Bundle Prerequisites, page 19](#)
- [Installing or Upgrading the Cisco VM-FEX Driver Software Bundle Using VUM, page 20](#)
- [Upgrading a Host to ESX or ESXi 4.0, Update 3 or to ESX or ESXi 4.1, Update 1 and the Compatible Cisco VM-FEX Driver Software Bundle, page 21](#)
- [Upgrading a Host to ESXi 5.0 and the Compatible Cisco VM-FEX Driver Software Bundle, page 23](#)
- [Upgrading a Host From ESXi 5.0 to ESXi 5.1 and the Compatible Cisco VM-FEX Driver Software Bundle, page 24](#)
- [Upgrading a Host to ESXi 5.1 and the Compatible Cisco VM-FEX Driver Software Bundle, page 25](#)
- [Installing or Upgrading the Cisco VM-FEX Driver Software Bundle on an ESX or ESXi Host, page 26](#)
- [Uninstalling the Cisco VM-FEX Driver Software Bundle, page 28](#)

Cisco VM-FEX Driver Software Bundle Installation Overview

To use the VM-FEX feature with Cisco UCS, you must install the Cisco UCS M81KR Virtual Interface Card in the Cisco UCS server and install the correct VMware ESX software version and Cisco VM-FEX Driver software bundle on it. The software that you install depends on whether you intend to use the VM-FEX feature in standard mode or high-performance mode. For more information, see [Cisco VM-FEX Driver Software Bundle Prerequisites, on page 19](#).

Cisco VM-FEX Driver Software Bundle Prerequisites

Before installing the Cisco VM-FEX Driver software bundle, make sure to satisfy these prerequisites:

- You must install a Cisco UCS Virtual Interface Card in the server you intend to use as the hypervisor host. For more information about installing Cisco UCS Virtual Interface Cards, see the *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.
- You must install the correct version of VMware ESX or ESXi software on the Cisco UCS Manager host. For VM-FEX in standard mode, you must install VMware ESX version 4.0, Update 1 software or later versions.
- You must obtain the Cisco VM-FEX Driver software bundle from the Cisco **Download Software** page:
 - For B-Series from, <http://software.cisco.com/download/navigator.html>. Select **Downloads Home > Products > Servers - Unified Computing > Cisco UCS B-Series Blade Server Software** and click **Unified Computing Systems (UCS) Drivers**. From this page, click **Latest Releases** or **All Releases** to select the release you want, and click **Download** to download the **ISO image of UCS-related drivers**.
 - For C-Series from, <http://software.cisco.com/download/navigator.html>. Select **Downloads Home > Products > Servers - Unified Computing > Cisco UCS C-Series Rack-Mount UCS-Managed Server Software** and click **Unified Computing Systems (UCS) Drivers**. From this page, click **Latest Releases** or **All Releases** to select the release you want, and click **Download** to download the **ISO image of UCS-related drivers**.
- You must install the correct version of the Cisco VM-FEX Driver software bundle on the hypervisor host. The Cisco VM-FEX Driver software bundle that you install depends on the VMware ESX or ESXi version you have installed on the hypervisor host. For information about the compatible versions of VMware ESX software and Cisco VM-FEX Driver software bundles, see VM-FEX Software Interoperability Matrix in *Hardware and Software Interoperability Matrix for B Series Servers* at http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html.

**Note**

The VEM software bundle is also a component of another product: the Cisco Nexus 1000V switch. Do not be concerned if you see references to this product during the installation of the VEM bundle. This reference is cosmetic only and does not affect the outcome of the installation and implementation of VM-FEX.

- You must be aware of any installation caveats. For information, see the *Release Notes for Cisco UCS Manager*.

Installing or Upgrading the Cisco VM-FEX Driver Software Bundle Using VUM

To install the Cisco VM-FEX Driver software bundle using VMware vSphere Update Manager (VUM), you need to log into the VMware vSphere client and copy the VM-FEX driver VIBs or bundles from cisco.com locally and import them in VUM.

For information about configuring VUM, see the VMware product documentation.

Upgrading a Host to ESX or ESXi 4.0, Update 3 or to ESX or ESXi 4.1, Update 1 and the Compatible Cisco VM-FEX Driver Software Bundle

You can use this procedure to upgrade a host to ESX or ESXi 4.0, Update 3 or 4.1, Update 1 and simultaneously upgrade the Cisco VM-FEX Driver software bundle.



Note

You can also perform this procedure using VMware VUM. For more information, see [Installing or Upgrading the Cisco VM-FEX Driver Software Bundle Using VUM](#), on page 20 and the VMware documentation.

Before You Begin

- You have copied the ESX or ESXi host software and Cisco VM-FEX Driver software bundle to the /tmp directory.

To determine the correct Cisco VM-FEX Driver software bundle for your ESX or ESXi version and Cisco UCS release, see the *Hardware and Software Interoperability Matrix for B Series Servers*.

Procedure

- Step 1** Power off the VMs or migrate all VMs to another host.
- Step 2** Migrate the vmk0 management interface to the vSwitch.
- Step 3** Remove the host from pass-through switching (PTS) mode.
- Step 4** If you are upgrading from ESX or ESXi 4.0, Update 1 to ESX or ESXi 4.0, Update 3, uninstall the VIB that enables pass-through switching (PTS). Otherwise, continue to step 6.
 - a) Enter the following command to identify the Cisco VM-FEX Driver VIB:
`esxupdate query --vib-view | grep cross_cisco | grep installed`
 The output appears showing the VIB package to be removed.
 - b) Enter the following command to remove the VIB.
`esxupdate -b VIB_package remove`

Example:

```
[root@serialport ~]# esxupdate query --vib-view | grep cross_cisco | grep installed
[root@serialport ~]# cross_cisco-vem-v100-esx_4.0.4.1.1.31-1.11.11 installed
2010-03-11T10:02:29.076573-05:00
[root@serialport ~]# esxupdate -b cross_cisco-vem-v100-esx_4.0.4.1.1.31-1.11.11 remove
```

- Step 5** If you are upgrading a host from ESX or ESXi 4.0, Update 1 to ESX or ESXi 4.0, Update 3, copy the ESX or ESXi Patch 04 (ESX400-201001001.zip) and the ESX or ESXi Patch 05 (ESX400-201003001.zip) to the /tmp directory and install them, if you have not already installed them. Otherwise, continue to step 6.
`vihostupdate --install --bundle "[path to VMware Update offline patch]" --server [vsphere host IP address]"`

Example:

```
[root@serialport ~]# vihostupdate --install --bundle "/tmp/Patch04/ESX400-201002001.zip"
--server 10.10.10.1
[root@serialport ~]# vihostupdate --install --bundle
"/tmp/Patch05/BuiltByVMware/ESX/20100330/ESX400-201003001.zip" --server 10.10.10.1
```

- Step 6** Go to the directory where the ESX or ESXi host software and Cisco VM-FEX Driver software bundle were copied.

Example:

```
[root@serialport ~]# cd tmp
[root@serialport tmp]#
```

- Step 7** Put the host in maintenance mode.

- Step 8** Enter the **vihostupdate** command:

```
vihostupdate --install --bundle "[path to VMware Update offline bundle]", "[path to Cisco updated VEM
offline bundle]" --server [vsphere host IP address]"
```

Example:

This example shows how to upgrade to ESX 4.0, Update 3 using the **vihostupdate** command from a client:

```
[root@serialport tmp]# vihostupdate --install --bundle
"/tmp/update-from-esx4.0-4.0_update03.zip", "/root/UPGRADE/BL/VEM400-201101406.zip --server
10.10.10.1
Enter username: root
Enter password:
Please wait installation in progress ...
The update completed successfully, but the system needs to be rebooted for the changes to
be effective.
[root@serialport tmp]#
```

Example:

This example shows how to upgrade to ESX 4.1, Update 1 using the **vihostupdate** command from a client:

```
[root@serialport tmp]# vihostupdate --install --bundle
"/tmp/update-from-esx4.1-4.1_update01.zip" , "/root/UPGRADE/BL/VEM410-201101407.zip" --server
10.10.10.1
Enter username: root
Enter password:
Please wait patch installation is in progress ...
The update completed successfully, but the system needs to be rebooted for the changes to
be effective.
```

- Step 9** Reboot the host.

- Step 10** Verify that the installation was successful. A successful installation shows the correct ESX or ESXi version and the correct Cisco VM-FEX Driver software bundle installed.

Example:

This example shows how to verify that the correct Cisco VM-FEX Driver software bundle was installed:

```
[root@serialport tmp]# esxupdate query --vib-view | grep cross_cisco | grep installed
cross_cisco-vem-vl30-esx 4.2.1.1.4.0.0-1.20.1 installed
2011-08-18T00:01:07.104096+00:00
[root@serialport tmp]# vmkload_mod -l | grep vem
vem-vl30-svs-mux 0x418035e73000 0x4000 0x417ff6d1fc40 0x1000 56 Yes
```



```
vem-v130-pts          0x418035e77000      0x16000      0x417ff6d193c0      0x1000      57 Yes
```

This example shows how to verify that ESX 4.0, Update 3 was installed:

```
[root@serialport tmp]# vmware -v
VMware ESX 4.0.0 build-398348
[root@serialport tmp]#
```

This example show how to verify that ESX 4.1, Update 1 was installed:

```
[root@serialport tmp]# vmware -v
VMware ESX 4.1.0 build-348481
[root@serialport tmp]#
```

- Step 11** Remove the host from maintenance mode.
- Step 12** Place the host in pass-through switching (PTS) mode.
- Step 13** Migrate the vmk0 management interface back to the host.
- Step 14** Power on the VMs or migrate all VMs back to the original host.

Upgrading a Host to ESXi 5.0 and the Compatible Cisco VM-FEX Driver Software Bundle

You can upgrade a host to ESXi 5.0 with the compatible Cisco VM-FEX Driver software bundle using an Interactive upgrade from CD, DVD, or USB drive or using VMware vSphere Update Manager (VUM) (also known as an online upgrade).

Before You Begin

You have copied the ESXi 5.0 host software and the Cisco VM-FEX Driver software bundle to the /tmp directory. To determine the correct Cisco VM-FEX Driver software bundle to use, see the *Hardware and Software Interoperability Matrix for B Series Servers*.

Procedure

- Step 1** Upgrade the Cisco UCS to release 1.4 and the ESX or ESXi host to one of the following releases:
 - Release 4.0, Update 3 with Cisco VM-FEX Driver software bundle v130-4.2.1.1.4.0.0-1.20.1.vib (or v129-4.2.1.1.4.0.0-1.20.1.vib if VUM was used)
 - Release 4.1, Update 1 with Cisco VM-FEX Driver software bundle v130-4.2.1.1.4.0.0-2.0.1.vib (or v129-4.2.1.1.4.0.0-2.0.1.vib if VUM was used)

For more information, see [Upgrading a Host to ESX or ESXi 4.0, Update 3 or to ESX or ESXi 4.1, Update 1 and the Compatible Cisco VM-FEX Driver Software Bundle](#), on page 21.

- Step 2** Upgrade the Cisco UCS to release 2.0.
For more information, see *Upgrading Cisco UCS from Release 1.4 to Release 2.0*.

- Step 3** Because VM-FEX for VMware has Cisco VM-FEX Drivers that require custom .vib files, create a custom ESX installable ISO file that includes the Cisco VM-FEX Driver software bundle. This custom ESX installable ISO file is installed as part of the ESXi 5.0 host upgrade.
For more information, see the "Upgrading Hosts That Have Third-Party Custom VIBs" section in the VMware *vSphere Upgrade* document for vSphere 5.0.
- Step 4** Upgrade the host to ESXi 5.0 and install the custom ESX installable ISO file.
For more information, see the VMware *vSphere Upgrade* document for vSphere 5.0.
- Note** You can also upgrade the host to ESXi 5.0 using VUM. For more information, see [Installing or Upgrading the Cisco VM-FEX Driver Software Bundle Using VUM](#), on page 20 and the VMware documentation.

Upgrading a Host From ESXi 5.0 to ESXi 5.1 and the Compatible Cisco VM-FEX Driver Software Bundle

You can upgrade a host to ESXi 5.1 with the compatible Cisco VM-FEX Driver software bundle using an Interactive upgrade from CD, DVD, or USB drive or using VMware vSphere Update Manager (VUM) (also known as an online upgrade).

Before You Begin

You have copied the ESXi 5.1 host software and the Cisco VM-FEX Driver software bundle to the /tmp directory. To determine the correct Cisco VM-FEX Driver software bundle to use, see the *Hardware and Software Interoperability Matrix for B Series Servers*.

Procedure

- Step 1** Upgrade the Cisco UCS to release 1.4 and the ESX or ESXi host to one of the following releases:
- ◦ Release 4.0, Update 3 with Cisco VM-FEX Driver software bundle v130-4.2.1.1.4.0.0-1.20.1.vib (or v129-4.2.1.1.4.0.0-1.20.1.vib if VUM was used)
 - Release 4.1, Update 1 with Cisco VM-FEX Driver software bundle v130-4.2.1.1.4.0.0-2.0.1.vib (or v129-4.2.1.1.4.0.0-2.0.1.vib if VUM was used)

For more information, see [Upgrading a Host to ESX or ESXi 4.0, Update 3 or to ESX or ESXi 4.1, Update 1 and the Compatible Cisco VM-FEX Driver Software Bundle](#), on page 21.

- Step 2** Upgrade the Cisco UCS to release 2.0.
For more information, see *Upgrading Cisco UCS from Release 1.4 to Release 2.0*.
- Step 3** Because VM-FEX for VMware has Cisco VM-FEX Drivers that require custom .vib files, create a custom ESX installable ISO file that includes the Cisco VM-FEX Driver software bundle. This custom ESX installable ISO file is installed as part of the ESXi 5.1 host upgrade.
For more information, see the "Upgrading Hosts That Have Third-Party Custom VIBs" section in the VMware *vSphere Upgrade* document for vSphere 5.1.

- Step 4** Upgrade the host to ESXi 5.1 and install the custom ESX installable ISO file.
For more information, see the VMware *vSphere Upgrade* document for vSphere 5.1.

Note You can also upgrade the host to ESXi 5.1 using VUM. For more information, see [Installing or Upgrading the Cisco VM-FEX Driver Software Bundle Using VUM, on page 20](#) and the VMware documentation.

Upgrading a Host to ESXi 5.1 and the Compatible Cisco VM-FEX Driver Software Bundle

You can upgrade a host to ESXi 5.1 with the compatible Cisco VM-FEX Driver software bundle using an Interactive upgrade from CD, DVD, or USB drive or using VMware vSphere Update Manager (VUM) (also known as an online upgrade).

Before You Begin

You have copied the ESXi 5.1 host software and the Cisco VM-FEX Driver software bundle to the /tmp directory. To determine the correct Cisco VM-FEX Driver software bundle to use, see the *Hardware and Software Interoperability Matrix for B Series Servers*.

Procedure

- Step 1** Upgrade the Cisco UCS to release 1.4 and the ESX or ESXi host to one of the following releases:
- ◦ Release 4.0, Update 3 with Cisco VM-FEX Driver software bundle v130-4.2.1.1.4.0.0-1.20.1.vib (or v129-4.2.1.1.4.0.0-1.20.1.vib if VUM was used)
 - Release 4.1, Update 1 with Cisco VM-FEX Driver software bundle v130-4.2.1.1.4.0.0-2.0.1.vib (or v129-4.2.1.1.4.0.0-2.0.1.vib if VUM was used)

For more information, see [Upgrading a Host to ESX or ESXi 4.0, Update 3 or to ESX or ESXi 4.1, Update 1 and the Compatible Cisco VM-FEX Driver Software Bundle, on page 21](#).

- Step 2** Upgrade the Cisco UCS to release 2.0.
For more information, see *Upgrading Cisco UCS from Release 1.4 to Release 2.0*.
- Step 3** Because VM-FEX for VMware has Cisco VEMs that require custom .vib files, create a custom ESX installable ISO file that includes the Cisco VM-FEX Driver software bundle. This custom ESX installable ISO file is installed as part of the ESXi 5.1 host upgrade.
For more information, see the "Upgrading Hosts That Have Third-Party Custom VIBs" section in the VMware *vSphere Upgrade* document for vSphere 5.0.
- Step 4** Upgrade the host to ESXi 5.1 and install the custom ESX installable ISO file.
For more information, see the VMware *vSphere Upgrade* document for vSphere 5.1.
- Note** If the installer displays the warning "DISTRIBUTED_VIRTUAL_SWITCH WARNING: Host contains DVS VIB(s) that have no substitute on the ISO," press **Enter** to continue.

Note You can also upgrade the host to ESXi 5.1 using VUM. For more information, see [Installing or Upgrading the Cisco VM-FEX Driver Software Bundle Using VUM, on page 20](#) and the VMware documentation.

During remediation when upgrading using VUM, check the check box for **Remove installed third-party software that is incompatible with the upgrade, and continue with the remediation.**

Installing or Upgrading the Cisco VM-FEX Driver Software Bundle on an ESX or ESXi Host

Use this procedure to install the Cisco VM-FEX Driver software bundle on a host.



Note

You can also perform this procedure using VMware VUM. For more information, see [Installing or Upgrading the Cisco VM-FEX Driver Software Bundle Using VUM, on page 20](#) and the VMware documentation.

Before You Begin

- You have copied the ESX or ESXi host software and Cisco VM-FEX Driver software bundle to the /tmp directory.

To determine the correct Cisco VM-FEX Driver software bundle for your ESX or ESXi version and Cisco UCS release, see the *Hardware and Software Interoperability Matrix for B Series Servers*.

Procedure

Step 1 Go to the directory where the ESX or ESXi host software and Cisco VM-FEX Driver software bundle were copied.

Example:

```
[root@serialport ~]# cd tmp
[root@serialport tmp]#
```

Step 2 If the host is at ESXi Release 5, proceed to step 3. If the host is at ESX or ESXi Release 4.0 or 4.1, do one of the following :

- If you are performing this installation or upgrade remotely from a client, put the host in maintenance mode and enter the **vihostupdate** command:

```
vihostupdate --install --bundle [path to desired offline Cisco VM-FEX Driver software bundle] --server
[vsphere host IP address]
```

Example:

The following examples shows how to install or upgrade a Cisco VM-FEX Driver software bundle remotely.

```
[root@serialport ~]# vihostupdate --install --bundle VEM400-201108405.zip --server 192.0.2.1
Enter username: root
Enter password:
Please wait patch installation is in progress ...
Host updated successfully.
```

- If you are performing this installation or upgrade locally on the ESX or ESXi host, log into the each host separately and, from the /tmp directory, use the **esxupdate** command to install the Cisco VM-FEX Driver software. This command loads the software manually onto the host, loads the kernel modules, and starts the Cisco VM-FEX Driver Agent on the running system.
esxupdate --bundle [VMware offline update bundle] update

Example:

The following example shows how to install or upgrade a Cisco VM-FEX Driver software bundle locally on a host.

```
~ # esxupdate -b cross_cisco-vem-v132-4.2.1.1.4.1.0-1.20.4.vib update
cross_cisco-vem-v132-4.2.1.1.4.1.0-1.20.4.vib
#####
[100%]

Unpacking cross_cisco-vem-v132-esx_4.2.1.1.4.1.0-1.20.4.vib
#####
[100%]

Installing packages :cross_cisco-vem-v132-esx_4.2.1.1.4.1.0-1.2..
#####
[100%]

Running [/usr/sbin/vmkmod-install.sh]...
ok.
```

Step 3 If the host is at ESXi Release 5.0, do one of the following:

- If you are performing this installation or upgrade remotely from a client, put the host in maintenance mode and enter the **esxcli** command, as follows:

```
esxcli --server Server-IP-Address software vib install --viburl URL-Path-to-vib
```

Example:

The following example shows how to perform this installation or upgrade remotely from a client.

```
# esxcli --server 30.20.41.197 software vib install --viburl
http://192.0.2.1/cross_cisco-vem-v132-4.2.1.1.4.1.0-3.0.4.vib
Enter username: root
Enter password:
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: Cisco_bootbank_cisco-vem-v132-esx_4.2.1.1.4.1.0-3.0.4
  VIBs Removed:
  VIBs Skipped:
```

- If you are performing this installation or upgrade locally on a host, log into the each host separately and from the /tmp directory, enter the following command:
esxcli software vib install -v /vib-file

Example:

The following example shows how to perform this installation or upgrade locally on a host.

```
# esxcli software vib install -v /cross_cisco-vem-v132-4.2.1.1.4.1.0-3.0.4.vib
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: Cisco_bootbank_cisco-vem-v132-esx_4.2.1.1.4.1.0-3.0.4
  VIBs Removed:
  VIBs Skipped:
```

Step 4 (Optional) Verify that the installation or upgrade of the Cisco VM-FEX Driver software bundle was successful on an ESX or ESXi 4.0, 4.1 or 5.0 host, by using the following commands:

```
esxcli software vib get | grep name
```

```
vmkload_mod -l |grep pts
```

Example:

The following example shows how to verify that the installation or upgrade of the Cisco VM-FEX Driver software bundle was successful on an ESX 4.1 host:

```
~ # esxupdate query --v |grep cisco
cross_cisco-vem-v132-esx_4.2.1.1.4.1.0-2.0.4          installed
2011-09-04T20:03:24.794110+00:00
~ # vmkload_mod -l |grep pts
mptsas                2      256
vem-v132-pts          0      132
~ #
#
```

Uninstalling the Cisco VM-FEX Driver Software Bundle

Use this procedure to uninstall the Cisco VM-FEX Driver software bundle from a host. The command that you use removes the software from the host, removes the kernel modules, and stops the VEM Agent on the running system.

Before You Begin

- Make sure that the host is not part of any DVS by removing all of the following active ports from the DVS:
 - VMware kernel NICs
 - Virtual switch interfaces
 - Virtual NICs
- You are logged in to the ESX or ESXi host remotely by using secure shell (SSH).

Procedure

- Step 1** If the host is at ESXi release 5.0, proceed to step 2. If the host is at ESX or ESXi release 4.0 or 4.1, uninstall the Cisco VM-FEX Driver software bundle by using the **esxupdate remove -b *VEM_name*** command.

Example:

The following example shows how to remove the Cisco VM-FEX Driver software bundle from a host that is at ESX or ESXi release 4.1:

```
[root@serialport ~]# esxupdate remove -b cross_cisco-vem-v132-esx_4.2.1.1.4.1.0-2.0.4
Removing cisco-vem-v132-esx
#####
[100%]

Running [/usr/sbin/vmkmmod-install.sh]...
ok.
[root@serialport ~]# esxupdate query --v |grep cisco
cross_cisco-vem-v132-esx_4.2.1.1.4.1.0-2.0.4                                uninstalled
2011-09-05T09:04:51.096141-07:00
[root@serialport ~]#
```

- Step 2** For an ESXi 5.0 host, uninstall the Cisco VM-FEX Driver software bundle by using the **esxcli software vib remove -n --maintenance-mode [*Cisco VM-FEX Driver bundle software name*]** command.

Example:

The following example shows how to remove the Cisco VM-FEX Driver software bundle from a host that is at ESXi release 5.0:

```
# esxcli software vib remove --maintenance-mode -n cisco-vem-v132-esx
Removal Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed:
  VIBs Removed: Cisco_bootbank_cisco-vem-v132-esx_4.2.1.1.4.1.0-3.0.4
  VIBs Skipped:
```

- Step 3** If the host is at ESXi release 5.0, proceed to step 4. If the host is at ESX or ESXi release 4.0 or 4.1, verify that the software was successfully uninstalled by checking the output of the **esxupdate query --v |grep cisco** command.

Example:

The following example shows how to verify that the Cisco VM-FEX Driver software bundle was successfully uninstalled from an ESX or ESXi release 4.1 host:

```
[root@serialport ~]# esxupdate query --v |grep cisco
cross_cisco-vem-v132-esx_4.2.1.1.4.1.0-2.0.4                                uninstalled
2011-09-05T09:04:51.096141-07:00
[root@serialport ~]#
```

- Step 4** For an ESXi 5.0 host, verify that the software was successfully uninstalled by checking for the output of the **esxcli software vib get | grep cisco** command.

Example:

```
~ # esxcli software vib get |grep cisco  
~ #
```

Step 5 Reboot the system.



Connecting Cisco UCS Manager to VMware vCenter

This chapter includes the following sections:

- [Connecting Using the Extension Key, page 31](#)
- [\(Optional\) Modifying the vCenter Extension Key, page 31](#)
- [Exporting a vCenter Extension File from Cisco UCS Manager , page 32](#)
- [Registering a vCenter Extension File in VMware vCenter, page 32](#)
- [\(Optional\) Configuring a Certificate for VM-FEX, page 33](#)

Connecting Using the Extension Key

(Optional) Modifying the vCenter Extension Key

You can modify the vCenter extension key to be more meaningful than the default ID string. This provides better system identification.

Procedure

- Step 1** In the **Navigation** pane, click the **VM** tab.
- Step 2** On the **VM** tab, expand the **All** node.
- Step 3** On the **VM** tab, click **VMWare**.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** In the **Actions** area, click **Modify Extension Key**.
- Step 6** In the **Modify Extension Key** dialog box, do the following:
 - a) In the **Key** field, modify the key as needed.

A vCenter extension key can have a maximum length of 33 characters. These characters can be letters, numbers, or hyphens. No other characters or spaces are permitted in the extension key.

- b) Click **OK**.

What to Do Next

Export the vCenter extension file or files from Cisco UCS Manager.

Exporting a vCenter Extension File from Cisco UCS Manager

Depending on the version of VMware vCenter you are using, you can either generate one extension file or a set of nine extension files.

Procedure

- Step 1** In the **Navigation** pane, click the **VM** tab.
- Step 2** On the **VM** tab, expand the **All** node.
- Step 3** On the **VM** tab, click **VMWare**.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** In the **Actions** area, click one of the following links:

Option	Description
Export vCenter Extension	For vCenter version 4.0 update 1 and later versions.
Export Multiple vCenter Extensions	For vCenter version 4.0.

- Step 6** In the **Export vCenter Extension** dialog box, do the following:
- In the **Save Location** field, enter the path to the directory where you want to save the extension file or files.
If you do not know the path, click the **...** button and browse to the location.
 - Click **OK**.
- Cisco UCS Manager generates the extension file(s) and saves them to the specified location.

What to Do Next

Register the vCenter extension file or files in VMware vCenter.

Registering a vCenter Extension File in VMware vCenter

In VMware vCenter, the vCenter extension files are called plug-ins.

Before You Begin

Export the vCenter extension file(s) from Cisco UCS Manager. Ensure that the exported vCenter extension files are saved to a location that can be reached by VMware vCenter.

Procedure

-
- Step 1** In VMware vCenter, choose **Plug-ins > Manage Plug-ins**.
- Step 2** Right-click any empty space below the Available Plug-ins section of the **Plug-in Manager** dialog box and click **New Plug-in**.
- Step 3** Click **Browse** and navigate to the location where the vCenter extension file(s) are saved.
- Step 4** Choose a vCenter extension file and click **Open**.
- Step 5** Click **Register Plug-in**.
- Step 6** If the **Security Warning** dialog box appears, click **Ignore**.
- Step 7** Click **OK**.
- The vCenter extension file registers as an available VMware vCenter plug-in. You do not need to install the plug-in; instead, leave it in the available state. If you are registering multiple vCenter extension files, repeat this procedure until all files are registered.
-

(Optional) Configuring a Certificate for VM-FEX

(Optional) Creating a Certificate for VM-FEX for VMware

Before You Begin

Copy a certificate to the fabric interconnect.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope cert-store	Enters system VM management VMware certificate store mode.
Step 5	UCS-A /system/vm-mgmt/vmware/cert-store # create certificate certificate-name	Creates the specified certificate for VM-FEX for VMware and enters system VM management VMware certificate store certificate mode.
Step 6	UCS-A /system/vm-mgmt/vmware/cert-store/certificate # set location {volatile workspace} path path certfile file-name	Specifies the location and filename of an existing certificate to use as the certificate for VM-FEX for VMware.

	Command or Action	Purpose
Step 7	UCS-A /system/vm-mgmt /vmware/cert-store/certificate # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to create a certificate for VM-FEX for VMware and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope cert-store
UCS-A /system/vm-mgmt/vmware/cert-store # create certificate VnLinkCertificate
UCS-A /system/vm-mgmt/vmware/cert-store/certificate* # set location workspace path /temp
certfile certificate.txt
UCS-A /system/vm-mgmt/vmware/cert-store/certificate* # commit-buffer
UCS-A /system/vm-mgmt/vmware/cert-store/certificate #
```

(Optional) Copying a Certificate to the Fabric Interconnect

Before You Begin

(Optional) Obtain a certificate.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# connect local-mgmt	Enters local management mode.
Step 2	UCS-A(local-mgmt)# copy <i>from-filesystem: [from-path]</i> <i>filename to-filesystem: [to-path]</i> <i>filename</i>	<p>Copies the certificate from its source location to its destination location. For the <i>from-filesystem:</i> argument, use one of the following syntax:</p> <ul style="list-style-type: none"> • ftp:// username@server-ip-addr • scp:// username@server-ip-addr • sftp:// username@server-ip-addr • tftp:// server-ip-addr : port-num <p>For the <i>to-filesystem:</i> argument, use one of the following syntax:</p> <ul style="list-style-type: none"> • Volatile: • Workspace:

The following shows how to use FTP to copy a certificate (certificate.txt) to the temp folder in the workspace:

```
UCS-A # connect local-mgmt
Cisco UCS 6100 Series Fabric Interconnect
```

TAC support: <http://www.cisco.com/tac>

Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained herein are owned by other third parties and are used and distributed under license. Some parts of this software may be covered under the GNU Public License or the GNU Lesser General Public License. A copy of each such license is available at <http://www.gnu.org/licenses/gpl.html> and <http://www.gnu.org/licenses/lgpl.html>

```
UCS-A(local-mgmt) # copy ftp://192.168.10.10/certs/certificate.txt
workspace:/temp/certificate.txt
UCS-A(local-mgmt) #
```

What to Do Next

Create a certificate for VM-FEX.

(Optional) Deleting a Certificate for VM-FEX for VMware

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope cert-store	Enters system VM management VMware certificate store mode.
Step 5	UCS-A /system/vm-mgmt/vmware/cert-store # delete certificate <i>certificate-name</i>	Deletes the specified certificate for VM-FEX for VMware.
Step 6	UCS-A /system/vm-mgmt/vmware/cert-store # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to delete a certificate for VM-FEX for VMware and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope cert-store
UCS-A /system/vm-mgmt/vmware/cert-store # delete certificate VnLinkCertificate
UCS-A /system/vm-mgmt/vmware/cert-store* # commit-buffer
UCS-A /system/vm-mgmt/vmware/cert-store #
```

(Optional) Deleting a Certificate for VM-FEX for VMware



CHAPTER 5

Configuring Distributed Virtual Switches in Cisco UCS

This chapter includes the following sections:

- [Distributed Virtual Switches, page 37](#)
- [Overview of Creating a DVS in Cisco UCS Manager, page 37](#)
- [Configuring a Distributed Virtual Switch, page 38](#)
- [Managing Distributed Virtual Switches, page 40](#)

Distributed Virtual Switches

The Cisco UCS distributed virtual switch (DVS) is a software-based virtual switch that runs along side the vSwitch in the ESX hypervisor and can be distributed across multiple ESX hosts. Unlike the vSwitch, which uses its own local port configuration, a DVS that is associated with multiple ESX hosts uses the same port configuration across all ESX hosts.

After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the VM-FEX for VMware implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.

Overview of Creating a DVS in Cisco UCS Manager

To create a distributed virtual switch (DVS) in Cisco UCS Manager, you must first create a vCenter, a datacenter under the vCenter, and a datacenter folder under the datacenter. You can then create a DVS in the datacenter folder. The vCenter name you specify in Cisco UCS Manager does not need to match the vCenter name specified in VMware vCenter; however, the datacenter name you specify in Cisco UCS Manager must match the datacenter name specified in VMware vCenter. The datacenter folder and DVS you create in Cisco UCS Manager are pushed to VMware vCenter.

Configuring a Distributed Virtual Switch

Before You Begin

You must first create a datacenter in VMware vCenter. Do not create the folder inside the datacenter or the DVS in VMware vCenter.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt /vmware # create vcenter vcenter-name	Creates the specified vCenter and enters system VM management VMware vCenter mode.
Step 5	UCS-A /system/vm-mgmt /vmware/vcenter # set hostname {hostname ip-addr}	Specifies the hostname or IP address of the remote vCenter Server instance associated to the vCenter object in Cisco UCS Manager. Note If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to local , configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to global , configure a DNS server in Cisco UCS Central.
Step 6	UCS-A /system/vm-mgmt /vmware/vcenter # set port port-num	The vCenter Server Port field specifies the HTTP port number of vCenter. The default port number is 80 and it is displayed in this field as default. Although the communication is HTTPS, vCenter receives the packets on its HTTP port. The valid range is 1-65355.
Step 7	UCS-A /system/vm-mgmt /vmware/vcenter # set description description	Provides a description for the vCenter. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks do not appear in the description field of any show command output.
Step 8	UCS-A /system/vm-mgmt /vmware/vcenter # create folder folder-name	(Optional) Creates the specified vCenter folder.

	Command or Action	Purpose
		Note A vCenter can contain multiple datacenters, none of which must be contained in a vCenter folder, so vCenter folders are optionally used only for organizational purposes.
Step 9	UCS-A /system/vm-mgmt /vmware/vcenter/ # create data-center <i>data-center-name</i>	Creates the specified datacenter and enters system VM management VMware vCenter datacenter mode. The datacenter name that you specify in Cisco UCS Manager must match the name of the datacenter previously created in VMware vCenter.
Step 10	UCS-A /system/vm-mgmt /vmware/vcenter/data-center # create folder <i>folder-name</i>	Creates the specified datacenter folder and enters system VM management VMware vCenter datacenter folder mode. Note At least one datacenter folder is required. You cannot create a distributed virtual switch (DVS) directly under a datacenter; you must create the DVS in a datacenter folder.
Step 11	UCS-A /system/vm-mgmt /vmware/vcenter/data-center/folder # create distributed-virtual-switch <i>dvs-name</i>	Creates the specified DVS and enters system VM management VMware vCenter datacenter folder distributed virtual switch mode.
Step 12	UCS-A /system/vm-mgmt /vmware/vcenter/data-center /folder/distributed-virtual-switch # { disable enable }	Disables or enables the DVS. If you disable the DVS, Cisco UCS Manager does not push any configuration changes related to the DVS to VMware vCenter.
Step 13	UCS-A /system/vm-mgmt /vmware/vcenter/data-center/folder /distributed-virtual-switch # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to create a vCenter, a datacenter with the exact same name as the datacenter in VMware vCenter, a DVS in the datacenter folder named Engineering, and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # create vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # set hostname 192.168.10.10
UCS-A /system/vm-mgmt/vmware/vcenter* # set port 1230
UCS-A /system/vm-mgmt/vmware/vcenter* # set description "vCenter running on my laptop"
UCS-A /system/vm-mgmt/vmware/vcenter* # create data-center MyDatacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # create folder Engineering
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder* # create distributed-virtual-switch
LabSwitch
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder/distributed-virtual-switch* # enable
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder/distributed-virtual-switch* #
commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder/distributed-virtual-switch #
```

Managing Distributed Virtual Switches

Adding a Folder to a vCenter

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt /vmware # scope vcenter vcenter-name	Enters system VM management VMware vCenter mode for the specified vCenter.
Step 5	UCS-A /system/vm-mgmt /vmware/vcenter # create folder folder-name	(Optional) Creates the specified vCenter folder and enters system VM management VMware vCenter folder mode. Note A vCenter can contain multiple datacenters, none of which must be contained in a vCenter folder, so vCenter folders are optionally used only for organizational purposes.
Step 6	UCS-A /system/vm-mgmt /vmware/vcenter/folder # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to add a vCenter folder named Lab 5 to the vCenter named MyVcenter and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # create folder Lab5
UCS-A /system/vm-mgmt/vmware/vcenter/folder* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/folder #
```

Adding a Datacenter to a vCenter

Before You Begin

You must first create a datacenter in VMware vCenter. Do not create the folder inside the datacenter or the DVS in VMware vCenter.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope vcenter vcenter-name	Enters system VM management VMware vCenter mode for the specified vCenter.
Step 5	UCS-A /system/vm-mgmt/vmware/vcenter # scope folder folder-name	(Optional) Enters system VM management VMware vCenter folder mode for the specified folder.
Step 6	UCS-A /system/vm-mgmt/vmware/vcenter/ # create data-center data-center-name	Creates the specified datacenter and enters system VM management VMware vCenter datacenter mode. The datacenter name that you specify in Cisco UCS Manager must match the name of the datacenter previously created in VMware vCenter.
Step 7	UCS-A /system/vm-mgmt/vmware/vcenter/data-center # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to add a datacenter named SQA-Datacenter to the vCenter named MyVcenter and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # create data-center SQA-Datacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center #
```

Adding a Folder to a Datacenter

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.

	Command or Action	Purpose
Step 4	UCS-A /system/vm-mgmt /vmware # scope vcenter <i>vcenter-name</i>	Enters system VM management VMware vCenter mode for the specified vCenter.
Step 5	UCS-A /system/vm-mgmt /vmware/vcenter # scope folder <i>folder-name</i>	(Optional) Enters system VM management VMware vCenter folder mode for the specified folder.
Step 6	UCS-A /system/vm-mgmt /vmware/vcenter/ # scope data-center <i>data-center-name</i>	Enters system VM management VMware vCenter datacenter mode for the specified datacenter.
Step 7	UCS-A /system/vm-mgmt /vmware/vcenter/data-center # create folder <i>folder-name</i>	Creates the specified datacenter folder and enters system VM management VMware vCenter datacenter folder mode.
Step 8	UCS-A /system/vm-mgmt /vmware/vcenter/data-center/folder # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to add a datacenter folder named SoftwareQA to the datacenter named MyDatacenter and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # scope data-center MyDatacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # create folder SoftwareQA
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder #
```

Deleting a Folder from a vCenter

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt /vmware # scope vcenter <i>vcenter-name</i>	Enters system VM management VMware vCenter mode for the specified vCenter.
Step 5	UCS-A /system/vm-mgmt /vmware/vcenter # delete folder <i>folder-name</i>	(Optional) Deletes the specified vCenter folder.

	Command or Action	Purpose
Step 6	UCS-A /system/vm-mgmt/vmware/vcenter # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to delete the vCenter folder named Lab5 from the vCenter named MyVcenter and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter # delete folder Lab5
UCS-A /system/vm-mgmt/vmware/vcenter* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter #
```

Deleting a Datacenter from vCenter

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope vcenter vcenter-name	Enters system VM management VMware vCenter mode for the specified vCenter.
Step 5	UCS-A /system/vm-mgmt/vmware/vcenter # scope folder folder-name	(Optional) Enters system VM management VMware vCenter folder mode for the specified folder.
Step 6	UCS-A /system/vm-mgmt/vmware/vcenter/ # delete data-center data-center-name	Deletes the specified datacenter. The datacenter name that you specify in Cisco UCS Manager must match the name of a datacenter previously created in vCenter Server.
Step 7	UCS-A /system/vm-mgmt/vmware/vcenter # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to delete the datacenter named SQA-Datacenter from the vCenter named MyVcenter and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # delete data-center SQA-Datacenter
```

```
UCS-A /system/vm-mgmt/vmware/vcenter* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter #
```

Deleting a Folder from a Datacenter

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope vcenter vcenter-name	Enters system VM management VMware vCenter mode for the specified vCenter.
Step 5	UCS-A /system/vm-mgmt/vmware/vcenter # scope folder folder-name	(Optional) Enters system VM management VMware vCenter folder mode for the specified folder.
Step 6	UCS-A /system/vm-mgmt/vmware/vcenter/# scope data-center data-center-name	Enters system VM management VMware vCenter datacenter mode for the specified datacenter.
Step 7	UCS-A /system/vm-mgmt/vmware/vcenter/data-center # delete folder folder-name	Deletes the specified datacenter folder.
Step 8	UCS-A /system/vm-mgmt/vmware/vcenter/data-center # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to delete the datacenter folder named SoftwareQA from the datacenter named MyDatacenter and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter # scope data-center MyDatacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center # delete folder SoftwareQA
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center #
```



Configuring Port Profiles

This chapter includes the following sections:

- [Port Profiles, page 45](#)
- [Creating a Port Profile, page 46](#)
- [Deleting a Port Profile, page 47](#)
- [Adding a Named VLAN to a Port Profile, page 48](#)
- [Deleting a Named VLAN from a Port Profile, page 49](#)
- [Port Profile Clients, page 49](#)
- [Adding a Port Profile Client to a Port Profile, page 50](#)
- [Deleting a Port Profile Client from a Port Profile, page 51](#)

Port Profiles

Port profiles contain the properties and settings that you can use to configure virtual interfaces in Cisco UCS for VM-FEX. The port profiles are created and administered in Cisco UCS Manager. After a port profile is created, assigned to, and actively used by one or more DVSEs, any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSEs.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to VMware vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile are visible in VMware vCenter. You must configure at least one port profile client for a port profile if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Creating a Port Profile

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope profile-set	Enters system VM management VMware profile set mode.
Step 5	UCS-A /system/vm-mgmt/vmware/profile-set # create port-profile <i>profile-name</i>	Creates the specified port profile and enters system VM management VMware profile set port profile mode.
Step 6	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set descr <i>description</i>	(Optional) Provides a description for the port profile. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks do not appear in the description field of any show command output.
Step 7	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set host-nwio-perf { high-performance none }	You can choose one of the following options: • high-performance • none
Step 8	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set max-ports <i>max-num</i>	Specifies the maximum number of ports that the port profile can use. The maximum number of ports that can be associated to a port profile is 4096. The default is 64 ports. If the DVS has more than one associated port profile, each port profile client can be set to use a maximum of 4096 ports.
Step 9	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set nw-control-policy <i>policy-name</i>	Specifies the network control policy to use for the port profile.
Step 10	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set pin-group <i>group-name</i>	Specifies the LAN pin group to use for the port profile.

	Command or Action	Purpose
Step 11	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set qos-policy <i>policy-name</i>	Specifies the QoS policy to use for the port profile.
Step 12	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # commit-buffer	Commits the transaction.

The following example shows how to create and configure a port profile named MyProfile and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # create port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set descr "This is my port profile"
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set host-nwio-perf high-performance
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set max-ports 24
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set nw-control-policy ncp5
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set pin-group PinGroup54
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set qos-policy QosPolicy34
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile #
```

What to Do Next

Add a port profile client to the port profile.

Deleting a Port Profile

You cannot delete a port profile if a VM is actively using that port profile.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope profile-set	Enters system VM management VMware profile set mode.
Step 5	UCS-A /system/vm-mgmt/vmware/profile-set # delete port-profile <i>profile-name</i>	Deletes the specified port profile.
Step 6	UCS-A /system/vm-mgmt/vmware/profile-set # commit-buffer	Commits the transaction. Cisco UCS Manager deletes the port profile and all associated port profile clients.

The following example shows how to delete the port profile named MyProfile and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # delete port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set #
```

Adding a Named VLAN to a Port Profile

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope profile-set	Enters system VM management VMware profile set mode.
Step 5	UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile <i>profile-name</i>	Enters system VM management VMware profile set port profile mode for the specified port profile.
Step 6	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # create vlan <i>vlan-name</i>	Specifies a named VLAN to use for the port profile. Note You can create multiple VLANs for guest VLAN trunking.
Step 7	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan # set default-net no	(Optional) Sets the default-net VLAN as the native VLAN in UCS Manager.
Step 8	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan # commit-buffer	Commits the transaction.

The following example shows how to add the VLAN named accounting to the port profile named MyProfile, set the VLAN as non-native, and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware# scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # create vlan accounting
```

```
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan* # set default-net no
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan #
```

Deleting a Named VLAN from a Port Profile

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope profile-set	Enters system VM management VMware profile set mode.
Step 5	UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile profile-name	Enters system VM management VMware profile set port profile mode for the specified port profile.
Step 6	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # delete vlan vlan-name	Deletes the specified named VLAN from the port profile.
Step 7	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # commit-buffer	Commits the transaction.

The following example shows how to delete the VLAN named accounting from the port profile named MyProfile and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware# scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # delete vlan accounting
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile #
```

Port Profile Clients

The port profile client determines the DVSEs to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSEs in the VMware vCenter. However, you can configure the client to apply the port profile to all DVSEs in a specific datacenter or datacenter folder or only to one DVS.

Adding a Port Profile Client to a Port Profile

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope profile-set	Enters system VM management VMware profile set mode.
Step 5	UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile <i>profile-name</i>	Enters system VM management VMware profile set port profile mode for the specified port profile.
Step 6	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # create client <i>client-name</i>	Creates the specified port profile client and enters system VM management VMware profile set port profile client mode. The port profile client determines the DVSES to which the port profile is applied. By default, a port profile applies to all DVSES in the vCenter; however, you can use the optional set data-center , set folder , and set dvs commands to apply the port profile to all DVSES in a specific datacenter, datacenter folder, or to a specific DVS.
Step 7	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set descr <i>description</i>	(Optional) Provides a description for the port profile client. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks do not appear in the description field of any show command output.
Step 8	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set data-center <i>data-center-name</i>	(Optional) Specifies the datacenter to which the port profile is applied.

	Command or Action	Purpose
Step 9	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set folder <i>folder-name</i>	(Optional) Specifies the datacenter folder to which the port profile is applied.
Step 10	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set dvs <i>name</i>	(Optional) Specifies the DVS to which the port profile is applied.
Step 11	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # commit-buffer	Commits the transaction.

The following example shows how to create a port profile client named OtherClient that applies the port profile named MyProfile to all DVSEs in the datacenter named OtherDatacenter and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # create client MyClient
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client* # set descr "This is my other
client for my port profile"
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client* # set data-center
OtherDatacenter
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client #
```

Deleting a Port Profile Client from a Port Profile

You cannot delete a port profile client if a VM is actively using the port profile with which the client is associated.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope profile-set	Enters system VM management VMware profile set mode.
Step 5	UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile <i>profile-name</i>	Enters system VM management VMware profile set port profile mode for the specified port profile.

	Command or Action	Purpose
Step 6	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # delete client <i>client-name</i>	Deletes the specified port profile client.
Step 7	UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # commit-buffer	Commits the transaction.

The following example shows how to delete the port profile client named OtherClient from the port profile named MyProfile and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware# scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # delete client OtherClient
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile #
```



Managing Pending Deletions of Distributed Virtual Switches

This chapter includes the following sections:

- [Pending Deletions of Distributed Virtual Switches, page 53](#)
- [Viewing Pending Deletions, page 54](#)
- [Viewing Properties for a Pending Deletion, page 54](#)
- [Changing Properties for a Pending Deletion, page 55](#)
- [Deleting a Pending Deletion, page 56](#)

Pending Deletions of Distributed Virtual Switches

When you delete a distributed virtual switch (DVS) from Cisco UCS Manager, either explicitly or by deleting any parent object in the hierarchy, Cisco UCS Manager initiates a connection with VMware vCenter to start the process of deleting the DVS. Until the DVS is successfully deleted from VMware vCenter, Cisco UCS Manager places the DVS in a pending deletion list.

However, Cisco UCS Manager cannot successfully delete a DVS from VMware vCenter if certain situations occur, including the following:

- VMware vCenter database was corrupted
- VMware vCenter was uninstalled
- The IP address for VMware vCenter was changed

If the DVS cannot be successfully deleted from VMware vCenter, the DVS remains in the pending deletion list until the pending deletion is deleted in Cisco UCS Manager or the properties for that pending deletion are changed in a way that allows the DVS to be successfully deleted from VMware vCenter. When you delete a pending deletion, the DVS is deleted from Cisco UCS Manager but is not deleted from VMware vCenter. If the DVS remains in VMware vCenter, you must delete the DVS manually.

You can view the pending deletion list, delete a pending deletion, or change the properties for a pending deletion in Cisco UCS Manager. For example, you can correct the VMware vCenter IP address for a pending

deletion so that Cisco UCS Manager can successfully initiate a connection and delete the DVS from VMware vCenter. You cannot cancel the deletion of a DVS from Cisco UCS Manager.

Viewing Pending Deletions

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # show pending-deletion	Displays the list of pending deletions.

The following example shows how to display the list of pending deletions:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # show pending-deletion
```

```
Pending Deletion:
  Id           Host           Distributed Virtual Switch
  -----
  1169232      192.168.10.10      LabDVS
  1176508      192.168.100.20     OpsDVS
  1176508      192.168.1.30       MyDVS
  1176508      192.168.1.40       OtherDVS
```

Viewing Properties for a Pending Deletion

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt/vmware # scope pending-deletion deletion-id	Enters system VM management VMware pending deletion mode for the specified pending deletion.

	Command or Action	Purpose
Step 5	UCS-A /system/vm-mgmt /vmware/pending-deletion # show detail	Displays the properties for the pending deletion.

The following example show how to display the properties for a specific pending deletion by using its assigned number, in this case, number 1169232:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope pending-deletion 1169232
UCS-A /system/vm-mgmt/vmware/pending-deletion # show detail

Pending Deletion:
  Id: 1169232
  vCenter: vCenterLab
  Host: 192.168.10.10
  Data Center Folder:
  Data center: Lab
  Folder: LabFolder
  Distributed Virtual Switch: LabDVS
  Extension key: Cisco-UCSM-b32cc112-83bb-11de-acc_7
  Certificate:
  Current Task: external VM manager deletion from local fabric
(FSM-STAGE:sam:dme:ExtvmmSwitchDelTaskRemoveProvider:RemoveLocal)
```

Changing Properties for a Pending Deletion

You can change the properties of a pending deletion, if necessary, to ensure that Cisco UCS Manager can successfully initiate a connection and delete the DVS from VMware vCenter.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt /vmware # scope pending-deletion deletion-id	Enters system VM management VMware pending deletion mode for the specified pending deletion.
Step 5	UCS-A /system/vm-mgmt /vmware/pending-deletion # set { certificate certificate-name data-center	Changes the specified property for the pending deletion.

	Command or Action	Purpose
	<i>data-center-name</i> data-center-folder <i>folder-name</i> folder <i>folder-name</i> host { <i>hostname</i> <i>ip-addr</i> }	Note If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to local , configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to global , configure a DNS server in Cisco UCS Central.
Step 6	UCS-A /system/vm-mgmt /vmware/pending-deletion # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to change the host IP address to 192.168.10.20 for a specific pending deletion, in this case, number 1169232 and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope pending-deletion 1169232
UCS-A /system/vm-mgmt/vmware/pending-deletion # set host 192.168.10.20
UCS-A /system/vm-mgmt/vmware/pending-deletion* # commit-buffer
UCS-A /system/vm-mgmt/vmware/pending-deletion #
```

Deleting a Pending Deletion

When you delete a pending deletion, the DVS is deleted from Cisco UCS Manager but is not deleted from VMware vCenter. If the DVS remains in VMware vCenter, you must delete the DVS manually.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt /vmware # delete pending-deletion <i>deletion-id</i>	Deletes the specified pending deletion.
Step 5	UCS-A /system/vm-mgmt /vmware # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to delete a specific pending deletion, in this case, number 1169232 and commit the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # delete pending-deletion 1169232
UCS-A /system/vm-mgmt/vmware* # commit-buffer
UCS-A /system/vm-mgmt/vmware #
```

